SISTEMA DE SEGURIDAD FÍSICA INTELIGENTE NORTE

PLIEGO DE PRESCRIPCIONES TÉCNICAS

ÍNDICE

ÍNDICE

1. INTRODUCCIÓN

1.1.OBJETO

El presente Pliego de Prescripciones Técnicas (PPT) establece el conjunto de requisitos técnicos que debe cumplir el contrato "Sistema de Seguridad Física Inteligente Norte", cuya finalidad es llevar a cabo el nuevo modelo de Seguridad Física de la Armada, que establece un entorno de seguridad único en el Área de Responsabilidad Norte como primera implementación del mismo, en el que los sistemas de seguridad física de todos los Entornos Globales de Seguridad (EGS) del Área deben estar interconectados y apoyados ante cualquier incidencia, en tiempo oportuno y de forma coordinada, por una unidad de reacción de la Fuerza de Protección de la Armada (FUPRO) debidamente dimensionada. Este sistema estará basado en la adaptación de una plataforma comercial existente optimizada para las diferentes instalaciones de la Armada.

1.2.SITUACION FUTURA

La situación a adoptar incluirá los siguientes elementos:

1.2.1. Centros Receptores de Alarmas Unificados

El **Centro Receptor de Alarmas Unificado** (en adelante **CRAU**), se plantea como un servicio de supervisión y gestión de la respuesta a incidentes de seguridad, centralizado en las unidades de área de responsabilidad Norte, donde existirá un CRAU, situado en la unidad de la FUPRO correspondiente a dicha área.

1.2.2. Centros Receptores de Alarma

Frente al CRAU podrán coexistir los Centros Receptores de Alarma (en adelante **CRA**), que pudiendo disponer de las mismas capacidades que aquel, presta servicio a una única unidad o entorno de seguridad, con guardia permanente 24/7. Podrán dotarse de la misma plataforma, con la salvedad de tener que ser remotado al CRAU con las características y sistemas que se consideren.

1.2.3. Centros de Control de alarmas remotadas

Podrán coexistir además los Centros de Control de alarmas remotadas (en adelante **C/C**), que disponen de algunas de las capacidades que prestan servicio a una única unidad, sin guardia permanente o con servicio no presente en ella. Podrán dotarse con un equipo que contempla la integración y gestión de las alarmas que posea, con la salvedad de tener que ser remotado al CRAU con las características y sub-sistemas que se consideren.

1.2.4. Plataforma Tecnológica de Gestión del Sistema de Seguridad Inteligente

La "Plataforma Tecnológica de Gestión del Sistema de Seguridad Inteligente" (en adelante "la plataforma") permitirá implementar el nuevo concepto de seguridad física de la Armada, sirviéndose del estado del arte de la tecnología existente en el mercado,

haciendo posible la implementación de centros de control, recepción y monitorización de señales de unidades localizadas en el área de responsabilidad Norte (ARN).
La plataforma debe dar soporte a las 5 funciones incluidas en el concepto de "seguridad": disuasión, detección, retardo, reconocimiento/evaluación y neutralización de posibles amenazas.
La plataforma contribuirá a la estrategia de mejora de la eficiencia de los procesos y optimización del uso de recursos, en base a capacidades como la automatización de tareas, la gestión por excepción, la gestión remota, y la gestión basada en datos.
Deberá ser capaz de gestionar los sub-sistemas establecidos en el punto 1.2.1., de un modo dinámico, estructurado, ágil y escalable, soportando las siguientes funciones y servicios:

- Modelado e implementación de procesos (motor de procesos de negocio, BPM), con posibilidad de modificarlos de manera dinámica.
- Visualización de video proveniente de los sistemas de video vigilancia.
- Automatización de acciones (por ejemplo, si se produce un evento de intrusión, posiciona una cámara domo apuntando a la zona, activa la iluminación de refuerzo, y reproduce una locución por megafonía).
- Tratamiento de información geoespacial (en 3D), con capacidad de presentar información, o de ofrecer al usuario un interfaz para la ejecución de acciones, de modo estático (por ejemplo, un edificio) y dinámico (posición en tiempo real de una patrulla móvil).
- Monitorización del estado de los sistemas integrados en la plataforma, con el fin de detectar cualquier condición que pueda comprometer su correcto funcionamiento, ya sea antes de que se materialice una degradación o pérdida de servicio, o una vez que esta se haya materializado en una incidencia.
- Gestión y simulación de escenarios, incidencias y eventos (entendiendo esto últimos como un conjunto de incidencias que de manera conjunta requieren un tratamiento distinto al que tendrían por separado).
- Gestión de alarmas. Clasificación, presentación, comunicación, escalado.
- Análisis y tratamiento de la información: cuadros de mando en tiempo real, informes automáticos, análisis interactivo de información, análisis y optimización de procesos (Smart Analytics).
- Aplicación de técnicas de inteligencia artificial y machine learning a los procesos de seguridad, de aplicación en ámbitos como el análisis de video, la detección de anomalías, o la predicción.
- Simulación de procesos, orientada a su prueba y depuración, y a la instrucción de usuarios.
- Debe soportar la implementación de los CRA del área de responsabilidad que le corresponda; y en su caso de los CRAU que se consideren, de manera dinámica (sujeta por ejemplo a horarios, niveles de alerta, o situaciones de emergencia) y jerárquica (posibilidad de que un CRAU asuma un nivel superior y englobe a uno o varios CRAU).
- El soporte a la implementación de procesos debe incluir tanto tareas de usuario (con su correspondiente interfaz) como tareas automáticas, soportadas en los subsistemas integrados.

- El interfaz de usuario debe abstraerlo de las implementaciones tecnológicas subyacentes (dispersión de tecnologías, fabricantes, etc.) y adecuarse a las funciones y competencias de cada usuario, ofreciéndolo un interfaz personalizado.
- Debe permitir la definición de niveles de seguridad que pueden estar asociados a una determinada ubicación o zona espacial, al nivel de alerta vigente, a un periodo temporal, a un evento (simple o complejo) o a una consigna manual.
- Debe permitir la implementación de procesos de gestión distribuida, de modo que la gestión de una unidad se pueda realizar desde distintas ubicaciones en función de horarios, capacidades de la unidad u otras condiciones, y mediante procesos de gestión híbridos.
- Debe soportar la monitorización local en horario laboral, y remota 24x7, la gestión de la reacción con capacidades propias o proporcionadas por otras unidades, en unidades dotadas de su CRA, o integradas en un CRAU externo.
- Debe soportar la segregación dinámica de zonas, activos, procesos y usuarios, y la transferencia de la responsabilidad de su gestión, permitiendo la gestión simultánea de distintas situaciones de emergencia bajo distintos ámbitos de responsabilidad. La gestión de la seguridad, sus procesos, activos, sistemas en un espacio geográfico determinado puede operar bajo un área de responsabilidad en condiciones normales.
- En caso de que se produzca una situación de emergencia, la plataforma debe permitir la segregación temporal y dinámica de ese espacio, pasando a gestionarse bajo dos ámbitos de responsabilidad distintos, gestionando sus propios activos y procesos de manera independiente.
- Debe permitir la movilidad de activos entre distintas zonas geográficas (por ejemplo, una cámara personal de las fuerzas de respuesta que se trasladan en un momento dado de la zona sur a la zona norte).
- Debe disponer de una completa gestión de roles, usuarios y permisos, de modo que cada usuario disponga de los permisos y del acceso a los recursos mínimos necesarios para el desarrollo de sus funciones.
- Debe soportar su utilización desde distintos tipos de dispositivos, fijos (equipo de escritorio o consola fija) o móviles (dispositivo personal o embarcado), y con las correspondientes particularidades asociadas a cada uno de ellos (comunicación por cable o inalámbrica, alimentación por red o por batería, distintos tamaños de pantalla, interfaz táctil, teclado y ratón, interacción visual y acústica, etc.). Ofrecerá un interfaz web, complementado con apps que faciliten su uso en dispositivos móviles.
- Debe soportar los protocolos de comunicación estándar y habitual en los procesos, sistemas y tecnologías empleados en el ámbito de las soluciones de gestión de la seguridad.
- Debe disponer de mecanismos que permitan un tratamiento adecuado de la seguridad de la información en sus distintos niveles (autenticación, autorización, y auditoría), protocolos de comunicación seguros, almacenamiento de información sensible cifrada y con alta disponibilidad.
- Debe dar soporte a los retos de dispersión geográfica y heterogeneidad de sistemas propios del entorno en el que se aplicará.
- Debe incorporar mecanismos de registro y trazabilidad de eventos.

1.2.5. Componentes principales del sistema y la interconexión entre ellos.

La integración de los distintos sistemas se realizará por medio de una única plataforma con capacidad para gestionarlos mediante inteligencia artificial, operarlos, controlarlos y supervisarlos de forma centralizada, sencilla y eficiente, incluyendo un histórico de incidencias.
La plataforma debe ser abierta (no depender de dispositivos específicos), flexible (integrar sistemas actuales y futuros), interoperable con todos los medios disponibles, modular, escalable (integrar futuras capacidades) y segura (en particular desde el punto de vista de la información).
Empleando esta misma plataforma se implementará un CRAU que integre los sistemas de seguridad física de los entornos de seguridad localizados de su AOR, de modo que permita su gestión centralizada y coordinada.
La plataforma permitirá aplicar inteligencia artificial a los procesos de gestión de la seguridad.
Capacidades y funciones del nuevo sistema.
Las funcionalidades del nuevo sistema serán las siguientes:

- Integración de todos los sistemas que componen el sistema de seguridad física.
- Interoperabilidad con diversos sistemas basada en estándares.
- La monitorización de todas las cámaras y alarmas en tiempo real.
- Motor de procesos sobre el que se implementen los procedimientos de seguridad en los que intervienen los usuarios del sistema y los sistemas integrados, pudiendo generarse a solicitud de un usuario o de forma automática ante un determinado evento mediante técnicas de inteligencia artificial.
- Análisis de correlación asociado a los procesos modelados.
- Capacidad de reacción automatizada o no según procedimientos en vigor.
- Integración de activos modulares sin limitación geográfica.
- Capacidad de simulación y adiestramiento sin perder la gestión real y efectiva.
- Capacidad de segregación y jerarquización tanto de sistemas como de los CRAU.
- Todos los elementos integrados (cámaras, grabadores, lectores de tarjetas, sensores, etc.) y las infraestructuras que permiten su funcionamiento (red de comunicaciones, sistemas de alimentación ininterrumpida, etc.) podrán ser monitorizados.
- Monitorización del sistema de control de accesos y capacidad de actuación sobre elementos físicos de control (tornos, puertas, barreras, etc.) de manera integrada con el sistema de video vigilancia.
- Gestión de los eventos de intrusión, el tratamiento de alarmas asociadas, o el envío de instrucciones de configuración para el armado o desarmado de elementos o zonas.
- Capacidad para captar datos asociados a procesos para su posterior análisis
- Tratamiento de alarmas asociadas a los eventos producidos por los sistemas integrados. Las alarmas se podrán comunicar por distintos medios y visualizar en la propia plataforma, en diversos formatos (ventanas emergentes, tablas, o en una visualización geo-referenciada) y con distintos procedimientos en función de su criticidad.

- Integración de sistemas de distintos fabricantes, ofreciendo un interfaz de acceso unificado para la gestión remota de distintas instalaciones.
- La integración de sistemas de video vigilancia permitiría por tanto el acceso al video en tiempo real, como a fragmentos de video o imágenes estáticas asociadas a eventos. Todo ello desde interfaces de usuario adaptados a las necesidades, tanto en un mapa donde se geo-localiza elementos, como desde vistas de mosaico o listados de ubicaciones.
- Todos los elementos integrados en la plataforma (cámaras, sensores de intrusión, etc.) podrán ser representados en un mapa en 2D o 3D. A su vez los elementos mostrados en el mapa podrán representar estados y alarmas cambiando de color, permitir el acceso a sus datos de estado y de motorización, y ofrecer la posibilidad de ejecutar acciones previamente configuradas, mediante un motor de procesos sobre el que se pueden implementar los procedimientos de la organización, en los que participen usuarios e intervengan también los sistemas integrados.
- Gestión de soluciones inteligentes con empleo de vehículos no tripulados (de superficie terrestre o marítima, aéreo o submarinos).

El proyecto debe desplegarse sobre la Infraestructura Integral de Información del Ministerio de Defensa (I3D), contemplando la posibilidad de integrar los sensores del **sistema** en una red 5G. Tal y como establece la estrategia 5G[1] del Ministerio de Defensa[2] como red de interconexión. Dicha estrategia contempla el uso de 5G para el ámbito operativo (C4ISTAR: Mando, Control, Comunicaciones, Computación, Inteligencia, Vigilancia, Adquisición de Objetivos y Reconocimiento) y en el resto de ámbitos funcionales y de apoyo Operativo (procesos logísticos y medioambientales, monitorización y mantenimiento remoto y predictivo de la infraestructura crítica, enseñanza y adiestramiento y sanidad). La red se encontraría bajo la Infraestructura Integral de Información del Ministerio de Defensa (I3D) y cumpliría los requisitos de seguridad de la información prefijados.

1.2.6. Áreas funcionales

La plataforma debe presentar un diseño multientornos, que incluya las siguientes funcionalidades:

- Entorno de interoperabilidad y adquisición de datos.

1 Una red 5G permite el funcionamiento de varias aplicaciones potenciales, entre las que cabe destacar: C2 (Mando y control), logística, mantenimiento, formación, inteligencia artificial (IA), realidad aumentada y virtual, sistemas ISR (Inteligencia, Vigilancia y Reconocimiento).

2 Resolución 307/08135/21, de 17 de mayo de 2021, de la Secretaria de Estado de Defensa, por la que se establece la Estrategia de comunicaciones móviles de quinta generación (Estrategia 5G) del Ministerio de Defensa.

- Entorno de persistencia.
- Entorno motor de procesos de negocio.
- Entorno procesador de eventos complejos.
- Entorno servidor de streaming de video.
- Entorno de monitorización.
- Entorno de alarmas.
- Entorno de actuación.
- Entorno de analítica.
- Entorno de presentación (interfaz de usuario).
- Entorno de informes.
- Entorno de gestión de usuarios.
- Entorno de gestión activos.
- Entorno de gestión de escenarios.
- Entorno de simulación.

Para la comunicación entre módulos existirá un bus de comunicación orientado a eventos, que implemente capacidades de publicación y suscripción a alta velocidad.

1.2.7. Entorno de implementación, actualización y pruebas del sistema

Deberá existir en la Oficina Técnica de Supervisión y Operación desde su creación un emulador de la plataforma que cumpla con las especificaciones contenidas en el ANEXO V y sea capaz de replicar a la misma con todas sus características y áreas funcionales de manera que permita:

- Desarrollo y modelado inicial del sistema.
- Probar actualizaciones y nuevas funcionalidades de la Plataforma Tecnológica de Gestión del Sistema de Seguridad Inteligente antes de llevarlas a los entornos de producción.
- Parametrización, prueba y optimización de procesos previa a su despliegue en producción.
- Procesos de homologación de soluciones de terceros para su integración en la Plataforma y en general, el Sistema de Seguridad Física Inteligente para garantizar su compatibilidad y correcta integración.
- Llevar a cabo acciones de formación a los futuros usuarios de la plataforma, ya sean perfiles de administración de la misma u operadores, con distintos perfiles funcionales.
- Probar nuevas versiones de software de control de la plataforma.
- Servir de back up de la última versión de software de la plataforma.
- Emular señales que se puedan recibir de los diversos componentes del sistema para realizar simulaciones y desarrollar protocolos de pruebas y procedimientos.

Este entorno incluirá los siguientes elementos:

- Sistema anti intrusión: incluirá los elementos que componen el sistema de control de intrusión, como por ejemplo el servidor, controladoras, y detectores (uno de cada tipología).

- Sistema de control de accesos: incluirá los elementos que componen el sistema de control de accesos, como por ejemplo el servidor, lectores/teclados, tarjeta controladora, elementos de control de puerta, elementos de acceso peatonal y elementos de acceso de vehículos.
- Sistema de megafonía e iluminación de disuasión: permitirá probar la funcionalidad de disuasión mediante emisión de locuciones por megafonía o encendido de iluminación.
- Sistema de videovigilancia: incluirá los componentes que componen el sistema de videovigilancia, como por ejemplo el servidor/grabador y cámaras (una de cada tipología).

Puestos de operador: equipado para emular el puesto de operador o jefe de sala del CRAU, CRA o CC, así como permitir la administración de todo entorno de implementación, actualización y pruebas del sistema. No forma parte del alcance el mobiliario.

- Pantallas de visualización: 2 pantallas de 50" conectadas a un ordenador, que emularán en este entorno la funcionalidad de un videowall del CRAU o CRA.
- Plataforma Tecnológica de Gestión del Sistema de Seguridad Inteligente: será una réplica funcional del entorno de producción. Incluirá tanto el software como el hardware sobre el que se ejecuta.
- Componentes necesarios para la instalación de los elementos que componen este entorno (rack, cableado eléctrico y de datos, soportes y anclajes, etc.).
  Estos elementos constituirás un entorno completamente aislado del entorno de producción, por lo que no podrán compartir con este ningún recurso.
  Se realizará una instalación que facilite la reubicación de los elementos físicos de forma sencilla (bien por reconfiguración de la sala donde se aloje este entorno, o bien por su traslado a otra ubicación).

1.2.8. Usuarios del sistema.

Se deben distinguir los siguientes perfiles de usuario:

- Usuario básico: personal de la dotación de la unidad que realiza tareas básicas de acreditación y manejo de credenciales.
- Usuario Avanzado: personal de la dotación de la unidad que realiza tareas avanzadas de acreditación, manejo de credenciales y extracción de informes.
- Usuario Operador: personal de seguridad que opera y monitorización del sistema.
- Usuario Administrador: personal que requiere conocimientos sobre las funcionalidades del sistema de seguridad física y las arquitecturas de los diferentes sistemas que los componen.
- Usuario Mantenedor: personal administrador de los sistemas para la realización de tareas de mantenimiento.

1.3. ALCANCE Y PLAZO

A la hora de establecer las fases, se tiene en cuenta el *Plan para el sistema de seguridad física inteligente de bases y arsenales*, firmado por el Almirante 2º Jefe del Estado Mayor de la Armada, de ahí que la numeración no sea correlativa.

El alcance incluye:

- El establecimiento de una oficina técnica.
- El suministro e implantación de un entorno de implementación, actualización y pruebas del sistema
- La realización de una adaptación inicial de la plataforma comercial en un número limitado de unidades.
- La extensión de la adaptación al resto de unidades de la AOR Norte.

Todo ello bajo las condiciones que se detallan en los siguientes apartados.

Es necesario disponer de una visión global que permita desarrollar un proyecto de seguridad física inteligente de bases y arsenales homogéneo en los distintas AOR, tanto en su ejecución como en su inversión económica y ciclo de vida posterior. En este sentido, la implementación del sistema de seguridad física inteligente de bases y arsenales se pretende realizar como sigue:

1.3.1. Fase 0.

Establecimiento y operación de una Oficina Técnica de Supervisión y Operación con las siguientes funciones:

- Dirección del proyecto.
- Entorno de implementación, actualización y pruebas del sistema, dedicado a:
  - Innovación y pruebas basadas en la plataforma.
  - Pruebas pre-producción.
  - Pruebas de soluciones a integrar en la plataforma.
  - Formación y adiestramiento.
- Modelado de procesos de seguridad para su modelado en la plataforma.
- Modelado para la identificación de activos y su modelado en la plataforma.
- Estudio para la identificación y modelado de *Key Performance Indicators* (KPIs).
- Estudio para la aplicación de técnicas de analítica avanzada de Inteligencia Artificial.
- Adecuación de los proyectos de los sistemas de seguridad de los distintos EGS de las instalaciones a integrar.
- Homologación de soluciones a integrar en la plataforma.
- Control de la configuración:
  - Supervisión técnica de usuarios.
  - Atención a usuarios.
  - Seguimiento continuo de la evolución del proyecto tras su implantación inicial.
- Acompañamiento posterior a la implementación: servicios de evolución, soporte y mantenimiento.
- Coordinación con la Oficina Técnica del I3D (CESTIC) para la red de comunicaciones en la que se integrará la plataforma.

Esta Oficina Técnica se ubicará en el Cuartel General de la Fuerza de Protección. Se simularán todos los requisitos establecidos en el entorno de implementación, actualización y pruebas del sistema allí existente, una vez validado se procederá a la siguiente fase.

1.3.2. Fase 1.

El alcance, según Apéndice A del Anexo III es el siguiente:

1.3.2.1. Diseño, instalación y puesta en funcionamiento del CRAU (sala de monitorización y operación) del AOR Norte (Tercio del Norte) :

- Puestos de supervisión y operación, incluyendo equipamiento informático y mobiliario.

- Video-Wall.

1.3.2.2. Adaptacion de la plataforma comercial del sistema de seguridad física inteligente de bases y arsenales que integre un número determinado de EGS del AOR Norte ubicados en Ferrol (TERNOR, ARFER, Polvorines de Mougá y Depósitos de Vispón) y la Escuela Naval Militar (Marín).

Este desarrollo incluirá

- Plataforma que lleve a cabo las siguientes funciones:
  - Integración en el sistema de seguridad de cada EGS:
    - Sub-sistema de video-vigilancia.
    - Sub-sistema de control de accesos.
    - Sub-sistema de detección de intrusión.
  - Capacidad de integración futura UAS terrestres, aéreos y de superficie, así como la capacidad de C-UAS en las EGS que se indiquen.
  - Monitorización de los sistemas.
  - Digitalización de procesos.
  - Cuadros de mando.
  - Informes.
  - Simulación.
  - Analítica avanzada de datos.
  - Aplicación de Inteligencia Artificial a la gestión de la seguridad.
- Centro de Proceso de Datos de soporte al CRAU:
  - Incluye:
    - Sistema de Alimentación Ininterrumpida (SAI).
    - Racks.
    - Cableado eléctrico y de comunicaciones.
    - Infraestructura de computación, almacenamiento, virtualización y orquestación de contenedores.
    - Gestión de la seguridad del CPD: video-vigilancia, control de accesos y detección de intrusión en el CPD.
    - Detección y extinción de incendios.
    - Gestión de la eficiencia energética del CPD.

Soporte y mantenimiento de la plataforma, CPD y los sistemas de seguridad de las EGS implicados:

- Mantenimiento:
    - Preventivo.
    - Correctivo.
    - Evolutivo.
    - Predictivo.
- Soporte a usuarios nivel 1.

1.4.2 Fase 2:

Desarrollo e implementación del sistema de seguridad física inteligente de bases y arsenales que integre el resto de los EGS del AOR Norte.

Incluirá la integración de los subsistemas de video vigilancia, control de accesos y anti intrusión en la Plataforma Tecnológica de Gestión del Sistema de Seguridad Inteligente.

A efectos de considerar su integración en la plataforma, el Apéndice B del Anexo III incluye la relación de unidades objeto de esta fase, los medios con que cuentan en la actualidad y los medios que está previsto incorporar para dar respuesta a las necesidades identificadas.

No forma parte del proyecto la renovación del equipamiento de estas unidades para cumplir los criterios de homogeneización y los requisitos de integración en la nueva plataforma.

1.3.3. En todas las fases:

La Oficina Técnica validará las soluciones a integrar en la plataforma.
Se incorporarán las soluciones implementadas en la correspondiente documentación de seguridad física (Entornos de Seguridad con Planes de Seguridad con el apoyo de las OSEF-Delegadas).

1.4. MANTENIMIENTO.

El licitador deberá incluir en su propuesta un plan de mantenimiento del sistema (completamente definido en el plan de aseguramiento de calidad) que incorpore, al menos, las siguientes actuaciones:

- **Hot-line.** Se deberá disponer de un servicio telefónico 24x7 que asistirá al usuario en las consultas que pudiese realizar sobre el uso de las aplicaciones que componen la plataforma. Además, dicho centro servirá para gestionar el servicio de mantenimiento, actuando como centro único de atención de incidencias. El coste de este servicio telefónico no podrá ser superior al de una llamada a una línea de abonado estándar. Se prohíben expresamente números de tarificación especial con

sobrecoste. El adjudicatario deberá realizar una propuesta que puede ser rechazada en caso de que no se considere acorde a las necesidades operativas.

- **Mantenimiento Preventivo.** Recogerá las tareas periódicas planificadas a desarrollar con el objeto de garantizar la continuidad del sistema antes de que se produzca una avería en la plataforma. Incluye las tareas de administración de sistemas, administración y tunning de base de datos, configuración de comunicaciones y aplicación de las políticas de seguridad y salvaguarda de información.
- **Mantenimiento Correctivo.** Consistente en corregir en las aplicaciones y/o los datos gestionados los errores de funcionamiento que se detecten en cualquiera de los componentes de la plataforma (hardware, software y comunicaciones), a excepción de las aplicaciones y sistemas que no pertenezcan directamente al sistema. Incluye la ejecución de los procesos necesarios para aplicar el parche de software o de datos: copia de seguridad, proceso de instalación, ejecución del proceso y prueba de la funcionalidad para comprobar que la corrección ha sido satisfactoria. Estas pruebas deberá realizarlas el contratista sin menos cabo de las que puedan realizar los usuarios que establezca Armada en la instancia de pruebas antes de su puesta en explotación. Se consideran incluidos todos los equipos, sistemas y comunicaciones que sean necesarios para garantizar los tiempos de respuesta y los niveles de calidad exigidos en este PPT a la plataforma.
- **Perfectivo.** Consistente en la modificación de las aplicaciones para adaptarlas a los cambios normativos y/o legislativos que pudiesen ocurrir durante la vigencia del contrato. Estas modificaciones se deberán llevar a cabo sobre todos los componentes de la plataforma (hardware, software y comunicaciones), al igual que en caso del mantenimiento correctivo, la implantación de las aplicaciones modificadas incluye la ejecución de los procesos: copia de seguridad, proceso de instalación, ejecución del proceso y prueba de la funcionalidad para comprobar que la corrección ha sido satisfactoria.
- **Evolutivo.** Consistente en la actualización periódica del software de la plataforma informática y de las librerías, run-times, software de comunicaciones, parametrizaciones de red, actualizaciones de software de dispositivos de red, adecuación de políticas de seguridad en routers, switches y firewalls, y cualquier otro módulos que se requiera para el funcionamiento de las aplicaciones que se propongan a través de la plataforma, de forma que todas la versiones de los software implicados se encuentren dentro de los estándares de la industria y con soporte técnico en vigor. Este proceso, que denominaremos migración de versión, incluye las tareas necesarias para:

  - ✓ Actualizar el sistema operativo de la plataforma base, si fuese necesario
  - ✓ Actualizar la versión del núcleo del gestor de base de datos, si fuese necesario
  - ✓ Actualizar la versión de las librerías, run-times y demás productos software empleados para la ejecución y puesta en explotación de las aplicaciones informáticas
  - ✓ Actualizar el código de las aplicaciones a las versiones del lenguaje compatibles con las nuevas versiones

- ✓ Transferir los datos desde el entorno antiguo al nuevo, transformando las estructuras que resulten necesarias
- ✓ Realizar las pruebas de cobertura funcional en el entorno nuevo
- ✓ Todos los procesos se realizarán en una instancia de pruebas hasta que resulte satisfactorio el plan de pruebas de cobertura funcional acordada
- ✓ La puesta en producción de la nueva plataforma informática y/o la nueva versión de las aplicaciones no se podrá realizar sin la conformidad expresa del responsable del contrato que nombre Armada
- ✓ Al finalizar el proceso, debe quedar una instancia de producción y una de pruebas idénticas y con todas las funcionalidades operativas
- ✓ Adaptar los interfaces de carga de datos y de integración con las aplicaciones de gestión de la Armada

La periodicidad con que se realicen actuaciones de mantenimiento evolutivo es muy relevante para la vigencia del soporte técnico de los productos hardware, software y de comunicaciones que componen la plataforma. Por otro lado, la Armada es consciente de que las versiones recién liberadas pueden tener errores que afectan al trabajo de los usuarios y a la comodidad del uso. Es por lo que se desea que las actuaciones de mantenimiento evolutivo se realicen sobre versiones que se consideren estables y lleven en el mercado, al menos, seis meses.

Todos los suministros y trabajos que resulten necesarios para realizar una migración de versión serán por cuenta del contratista, no pudiendo resultar ningún cargo a la Armada por este concepto. Bastará con que uno sólo de los componentes de la plataforma: hardware, software o de comunicaciones; tenga fecha anunciada para la caducidad del soporte técnico que presta el fabricante para que el contratista esté obligado a programar y realizar una migración de versión de forma que todos los componentes mantengan el servicio de mantenimiento del fabricante en vigor.

Es responsabilidad del contratista la realización de las tareas técnicas necesarias para el correcto funcionamiento de los aplicativos implantados en la plataforma, salvaguardar los datos y garantizar que los tiempos de respuesta a las solicitudes de servicio que reciba la plataforma sean adecuados a lo estipulado en este documento. Para ello, forma parte del alcance del presente contrato realizar las tareas de mantenimiento preventivo, correctivo, perfectivo y evolutivo que resulten necesarias durante la duración del mismo.

La propuesta presentada deberá incluir y/o detallar, al menos, los siguientes aspectos:

- ➢ Los tiempos de respuesta (no pueden ser superiores a los solicitados en el presente PPT)

- Una descripción detallada de los procedimientos y funciones para la realización de los tipos de mantenimiento considerados

- Se deberá indicar si las funciones de mantenimiento serán realizadas por personal propio o subcontratado con otra empresa. En cualquier caso se especificará si se posee delegación en las ubicaciones de las instalaciones de la Armada objeto del presente suministro o alrededores y en ese caso si el personal adscrito a las mismas es el que desarrollará las funciones.

El licitador deberá incluir en su propuesta una relación de los servicios durante los **12 meses** siguientes a la finalización de este contrato achacables a un defecto en la implantación no encuadrable en la garantía y ajeno a la Armada.

A partir de los 12 meses iniciales, en el caso de que la Armada desee renovar el contrato de mantenimiento con el adjudicatario de los trabajos, éste tendrá que asumir dicha renovación, sin potestad para rechazarla y con derecho a un incremento del importe proporcional a lo pagado anteriormente.

No se incluye dentro del alcance del mantenimiento el suministro de repuestos de equipos.

Tiempos de respuesta

Para determinar los tiempos de respuesta máximos admisibles para el mantenimiento correctivo es conveniente aclarar previamente los siguientes conceptos:

- **Tiempo de respuesta:** Se define el tiempo de respuesta como el periodo transcurrido desde que la Armada notifica una incidencia al centro de atención (Hot-Line), hasta que el servicio técnico del mantenedor se pone en contacto con la Armada.

- **Tiempo de resolución in-situ:** Tiempo que transcurre desde la notificación de una incidencia por parte de la Armada hasta que el servicio técnico del mantenedor se persona en las instalaciones de la Armada para intentar su resolución.

- **Tiempo de resolución remota:** Tiempo que transcurre desde la notificación de una incidencia por parte de la Armada hasta que el servicio técnico del mantenedor intenta la resolución remota de la misma sin necesidad de acudir a las instalaciones de la Armada.

- **Avería crítica:** Aquella que supone la falta de operatividad total del sistema o de los subsistemas de gestión de procesos, gestión de medios y/o gestión de escenarios.

- **Avería no crítica:** Falta de operatividad en alguno de los subsistemas no contemplados dentro de la avería crítica.

Los tiempos máximos de respuesta admisibles en este expediente son:

- **Incidencia crítica:**
  - ✓ Tiempo máximo de respuesta: 10 minutos.
  - ✓ Tiempo máximo de resolución remota: 1 hora.
  - ✓ Tiempo máximo de resolución in-situ: 4 horas. En el caso de averías hardware, si se le da una solución parcial y previa aceptación de la Armada, este tiempo podrá ser ampliado a 72 horas.
- **Incidencia no crítica:**
  - ✓ Tiempo máximo de respuesta: 10 minutos.
  - ✓ Tiempo máximo de resolución remota: 24 horas.
  - ✓ Tiempo máximo de resolución in-situ: 72 horas. En el caso que se le dé una solución parcial y previa aceptación de la Armada, este tiempo podrá ser ampliado a 7 días.

1.5.OFICINA TÉCNICA OFICINA DE SUPERVISION Y OPERACION

A continuación, se detalla el alcance de los servicios a proporcionar por la Oficina Técnica de Supervisión y Operación:

1.5.1. Funciones y responsabilidades

1.5.1.1. Dirección del proyecto.

El servicio de Oficina Técnica de Supervisión y Operación ejercerá las funciones de dirección de proyecto por parte del adjudicatario.

1.5.1.2. Gestión de un entorno de implementación, actualización y pruebas del sistema

El adjudicatario ejercerá las labores de gestión de un entorno de implementación, actualización y pruebas del sistema, compuesto por un subsistema de hardware y software que permita desarrollar las siguientes actividades:

- Adaptación y pruebas basadas en la plataforma.
- Pruebas pre-producción.
- Pruebas de soluciones a integrar en la plataforma.
- Formación y adiestramiento.

Se engloban en este ámbito funciones tales como:

- La gestión de los recursos del laboratorio: incluye la disposición efectiva de los distintos sistemas en estado operativo, realizando la parametrización necesaria para cada caso, y el mantenimiento de los sistemas asociados.

- La coordinación de actividades: incluye la elaboración y mantenimiento de una planificación en el tiempo de los distintos usos previstos.

- La coordinación con los distintos usuarios del laboratorio: incluye la gestión de usuarios (alta, baja, modificación), la difusión de las normas de uso y la realización de planificaciones acordes a las necesidades y disponibilidad del laboratorio.

1.5.1.3. Estudio de procesos de seguridad para su modelado en la plataforma.

El adjudicatario llevará a cabo los estudios necesarios para la digitalización de los procesos de seguridad de la organización sobre la plataforma.

Partiendo de la documentación de los procesos de la organización, el adjudicatario elaborará una propuesta de implementación alineada con la estrategia de gestión de la seguridad inteligente y las capacidades de la plataforma y subsistemas integrados.

Dicha propuesta incluirá:

- Documento explicativo del proceso y solución adoptada.
- Flujograma del proceso en notación BPMN.
- Diseño de interfaces de usuario.
- Diseño del modelo de datos.
- Diseño de integraciones de los subsistemas implicados.
- Plan de pruebas.
- Plan de formación.

1.5.1.4. Validación de soluciones a integrar en la plataforma.

La Oficina Técnica de Supervisión y Operación se encargará de la validación de cualquier solución con carácter previo a su integración en la plataforma. Dicha homologación incluirá:

- Estudio previo de compatibilidad.
- Colaboración con fabricantes e integradores de las soluciones a integrar, para la resolución de las dudas que pueda tener cualquiera de las partes.
- Colaboración en el diseño y ejecución de planes de pruebas.

- Elaboración de informe de conclusiones relativo a la integración de la solución en la plataforma.

- Protocolo de pruebas en el Hardware del entorno de implementación, actualización y pruebas del sistema de la Oficina Técnica de Supervisión y Operación.

1.5.1.5. Control de configuración.

El adjudicatario diseñará y ejecutará un plan de control de la configuración acorde a las necesidades del proyecto. Dicho plan deberá dar respuesta a las necesidades de difusión, formación, atención a usuarios, y seguimiento de la evolución del proyecto.

La elaboración del plan tendrá en cuenta los distintos usuarios de los sistemas, así como otros interesados implicados en el proyecto.

Previa a la elaboración del plan el adjudicatario deberá realizar un diagnóstico de aquellos aspectos que puedan influir en la gestión del cambio.

1.5.1.6. Acompañamiento posterior a la implementación: servicios de evolución, soporte y mantenimiento.

La Oficina Técnica de Supervisión y Operación será la encargada de la gestión y prestación de los servicios de soporte y mantenimiento, con los requisitos establecidos en el correspondiente apartado de este documento.

1.5.1.7. Coordinación con la Oficina Técnica del I3D (CESTIC) para la red de comunicaciones en la que se integrará la plataforma.

La Oficina Técnica de Supervisión y Operación del proyecto deberá colaborar con la Oficina Técnica del I3D para todas aquellas cuestiones del proyecto que puedan entrar en el alcance de la I3D. Dicha colaboración se concreta en aspectos como:

- Conocimiento del proyecto I3D, su alcance y planificación.

- Identificación de necesidades de este proyecto que puedan estar condicionadas por el I3D. Elaboración de peticiones a la oficina técnica del I3D.

- Coordinación de iniciativas del I3D que afecten al desarrollo del proyecto.

1.5.1.8. Otras funciones

La Oficina Técnica de Supervisión y Operación deberá realizar los cometidos propios de las siguientes consultorías/asistencias:

- Identificación de activos y su modelado en la plataforma.
- Identificación y modulado de Key Performance Indicators (KPIs).
- Aplicación de técnicas de analítica avanzada de Inteligencia Artificial.

- Elaboración de los proyectos de los sistemas de seguridad de los distintos EGS a integrar.

1.6. NECESIDAD DE CONOCER DEL FUTURO CONTRATISTA

El futuro contratista deberá de conocer:

- Los sistemas actuales del Sistema de Seguridad del AOR Norte (Sistemas de video vigilancia, control de accesos, detección de intrusión, iluminación de seguridad, Control de Accesos, Alarmas, etc.).
- Los procedimientos operativos en vigor.
- La documentación clasificada en vigor que se indique.

2. MATERIALES Y MEDIOS A SUMINISTRAR POR LA ARMADA

La Armada podrá dar acceso al contratista, previo el control correspondiente y según sus procesos internos de seguridad, a las unidades que integren los sistemas definidos en el punto 1.5 de este documento.

Así mismo, la Armada podrá dar acceso a los procedimientos operativos, documentación clasificada y otros elementos que hayan sido definidos en el apartado 1.5 de este documento. La entrega de la documentación se realizará según la normativa vigente de seguridad.

3. NORMATIVA APLICABLE Y DOCUMENTACIÓN DE REFERENCIA

3.1. DOCUMENTOS APLICABLES DE CARÁCTER GENERAL

Los documentos aplicables, en su última versión aprobada, son los que se citan a continuación:

3.2. DOCUMENTOS DE REFERENCIA PROPIOS DEL SISTEMA

3.2.1. Generales

Las restricciones serán las derivadas del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como de lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Normas específicas de la Comunidad Autónoma y del Municipio donde se ubican las instalaciones.

Todas aquellas Normas que por la pertenencia de España a la Unión Europea sean de obligado cumplimiento en el momento de la presentación del Proyecto Constructivo.

En todo caso deberán acreditarse:

- Certificación ISO 9001 o equivalente – Sistemas de Gestión de la Calidad.

- Certificación ISO 14001 o equivalente – Sistemas de Gestión Ambiental.

- Certificación ISO 27001 o equivalente – Sistemas de gestión de Seguridad de la Información.

- Certificación ISO 20000-1 o equivalente – Gestión de servicios de tecnologías de la información

- Certificación ISO 45000-1 o equivalente – Gestión de servicios de seguridad y salud en el trabajo.

3.2.2. Seguridad Física

Seguridad documental.

OR-ASIP-04-01.04 Orientaciones para el Manejo de Información Clasificada con Grado de Difusión Limitada. ONS

Seguridad en el personal.

OR-ASIP-04-02.02 – Instrucción de Seguridad del Personal para acceso a Información Clasificada. ONS

Seguridad física.

OR-ASIP-01-01.03 Orientaciones para el Plan de Protección de una Zona de Acceso Restringido. ONS

OR-ASIP-01-02.03 Orientaciones para la Constitución de Zonas de Acceso Restringido.

Seguridad de los Sistemas de Información y Comunicaciones. ONS

OR-ASIP-03-01.04 Orientaciones para la Acreditación de Sistemas de Información y Comunicaciones para el manejo de Información Clasificada. Serán de aplicación todas las normas relativas a la seguridad documental, personal, física y de los sistemas de información y comunicaciones, que estén en vigor en el momento de la puesta en marcha del sistema. ONS

NORMA NS/03. Seguridad Física. ONS

IPSEG Nº308. Acreditación de las Zonas de Acceso Restringido. 2º AJEMA.

IPSEG Nº 102 Normas, criterios, medios y procedimientos para la Seguridad física en las unidades. 2º AJEMA.

3.2.3. Seguridad de la Información

- Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa (AG CIS/TIC), marzo 2017.

- Instrucción Técnica 01/14: Arquitectura Técnica Unificada del Ministerio de Defensa Versión 3.0.

- Política de certificación del Ministerio de Defensa PO-345-SEGINFO/01/14/V1, especialmente para los formatos de Perfil de Certificado, Extensiones e Identificadores de objeto.

- Instrucción técnica de requisitos de integración en la plataforma SOA del MINISDEF IT-01/SDGTIC/11/GRIPS/V.1

- GU-345-ARTEC/02/13/V2.1 Guía de uso de los servicios WEB de DICODEF.

- ES-345-CAL/01/2012 "Especificaciones de integrabilidad".

- Ministerio de Defensa - SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa (PECIS), octubre 2018.

- Metodología MÉTRICA Versión V3.

- Certificación GS1 AECOC XML v2.0.

- RFC 2460 - Internet Protocol Version 6 (IPv6) Specification.

- Series CCN-STIC XXX (año 2015) aplicables al entorno tecnológico definido en el presente PPT.

3.2.4. Normativa de Calidad

- PECAL2110 "Requisitos OTAN de Aseguramiento de la Calidad para el Diseño/ Desarrollo y Producción" (excepto punto 9 de la norma).

- PECAL2210 "Requisitos OTAN de Aseguramiento de la Calidad del Software, Suplementarios a la PECAL 2110 o la PECAL 2310.

- PECAL 2105"Requisitos OTAN para planes de calidad entregables".

- IT 4201.05C "Instrucción Técnica para la elaboración y evaluación de planes de calidad según PECAL 2105 y PECAL 2210".

- CMMI Level 3 (Capability Maturity Model® Integration Level 3).

3.3. DOCUMENTOS DE REFERENCIA SOBRE RIESGOS LABORABLES

Los documentos de referencia sobre riegos laborables, en su última versión aprobada, son los que se citan a continuación:

- Ley 31/ 1995, de 8 de noviembre, de Prevención de Riesgos Laborales.
- Real Decreto 171/ 2004, de 30 de enero, por el que se desarrolla el artículo 24 de la Ley 31/ 1995, de 8 de noviembre, de Prevención de Riesgos Laborales, en materia de coordinación de actividades empresariales.
- Ley de Higiene y Seguridad en el Trabajo. (RD 486/ 1997 de 14 de Abril y 485/ 1997 de 14 de Abril).

- Real Decreto 1932/ 1998, de 11 de septiembre, de adaptación de los capítulos III y IV de la Ley 31/ 1995, de 8 de noviembre, de Prevención de Riesgos Laborales, al ámbito de los centros y establecimientos militares.
- Ley 31/ 1995, de 8 de noviembre, de Prevención de Riesgos Laborales.
- Real Decreto 486/1997, de 14 de abril, por el que se establecen las disposiciones mínimas de seguridad y salud en los lugares de trabajo.
- Real Decreto 488/1997, de 14 de abril, sobre disposiciones mínimas de seguridad y salud relativas al trabajo con equipos que incluyen pantallas de visualización.

3.4. DOCUMENTOS DE REFERENCIA SOBRE EL APOYO LOGÍSTICO

La configuración logística de los sistemas y equipos adquiridos por la Armada en este contrato se elaborará de acuerdo a lo dispuesto en la Instrucción Permanente de sostenimiento número 2/2016 de 17 de noviembre de 2016 del Almirante Jefe del Apoyo Logístico sobre la configuración de las unidades.

4. REQUERIMIENTOS DEL SISTEMA

4.1. ESPECIFICACIONES TÉCNICAS

- ES_001: La plataforma debe contar con una arquitectura distribuida basada en micro servicios.
- ES_002: Su diseño estará orientado a su despliegue en tecnología de contenedores que permita escalabilidad, confiabilidad y garantice un mejor soporte y evolución tecnológica. El software de orquestación de contenedores, permitirá balancear la carga de trabajo y garantizar la alta disponibilidad de la plataforma.
- ES_003: Deberá implementar una arquitectura orientada a eventos (paradigma publicación-suscripción).
- ES_004: Su diseño debe garantizar:
  - 004.1.La evolución futura, integrando nuevas funciones y servicios, permitiendo incorporar en cada momento el estado del arte de la tecnología, mediante una arquitectura modular escalable, considerando que debe tener un ciclo de vida mínimo de 8-10 años.
  - 004.2. Asimismo, se permitirá la evolución incremental, esto es, que se evolucionen partes de la solución y sustitución de las mismas por piezas tecnológicas más avanzadas.
  - 004.3. La interoperabilidad con otros sistemas mediante estándares, evitando las integraciones propietarias en la medida de lo posible. Dicha interoperabilidad en su mayor parte se basará en contratos de interoperabilidad gestionados y mantenidos en el sistema, Eventos o API.
  - 004.4. El tratamiento de grandes volúmenes de datos (big data).
  - 004.5. La robustez y tolerancia a fallos (alta disponibilidad).
  - 004.6. La escalabilidad en cuanto a número de usuarios, subsistemas integrados, áreas de responsabilidad, etc.
  - 004.7. Capacidad de Autenticación integrada con los sistemas corporativos (Single Sign On).
  - 004.8. Gestión de Usuarios y Roles escalonados para permitir distintas operativas.

- 004.9. Capacidad de Despliegue on-premise y en Plataforma como Servicio (PaaS).
- 004.10. Integración y monitorización IoT basada en estándares de la industria.
- 004.11. La arquitectura de la misma debe basarse en contenedores y orquestación de los mismos, de forma que escale de manera automática para poder cumplir con los requisitos de una plataforma de seguridad de tener una Disponibilidad máxima.
- 004.12. Capacidad de despliegue, operación y mantenimiento remoto, tanto en proveedores cloud como on-premise.
- 004.13. Protocolos de seguridad en las integraciones IoT con un nivel ENS medio.
- 004.14. Uso de certificados SSL y otros métodos de autenticación que permitan comprobar la veracidad del sistema.
- 004.15. Registros de auditoría sobre las acciones realizadas por los usuarios.
- 004.16. Trazabilidad en logs y gestión de los mismos.
- 004.17. Capacidad de monitorización y alertado sobre la propia infraestructura.
- 004.18. Capacidad de observabilidad siguiendo los principios y estándares de la industria.

– ES_005: Producto comercial. La plataforma tecnológica de soporte al CRAU debe ser un producto comercial, que garantice su madurez, sostenibilidad y evolución futura. No se admitirán propuestas basadas en desarrollo a medida. Este punto deberá acreditarse mediante la entrega de un video en el que se muestre un resumen de las principales funcionalidades, y la puesta a disposición de un entorno de demo.

ES_005: El proyecto debe desplegarse sobre la Infraestructura Integral de Información del Ministerio de Defensa (I3D), contemplando la posibilidad de integrar los sensores del sistema en una red 5G.

ES_006: Del sistema de control de accesos:

La Plataforma Tecnológica de Gestión del Sistema de Seguridad Inteligente deberá integrar las capacidades de:

- 006.1. Identificación biométrica para el acceso peatonal, mediante otros sistemas y que contemple la manipulación manual del control.
- 006.2.Identificación de las matrículas vehículos
- 006.3. Gestión de ocupantes de los vehículos.

En todo momento, se debe conocer el número de personas y de vehículos que se encuentran dentro de la unidad. En Arsenales y Bases Navales se deberá contemplar la salida y la llegada a la mar de los diferentes buques o aeronaves.

ES_007: Del Sistema de video vigilancia:

La Plataforma Tecnológica de Gestión del Sistema de Seguridad Inteligente deberá integrar las capacidades de:

- 007.1. Reconocimiento de objetos, merodeo de personas, vehículos (matrículas, número de ocupantes) que se sitúen o estacionen en el perímetro de seguridad

- 007.2. Detección de intentos de intrusión según la norma UNE-EN 50131-1 o equivalente en vigor.

- 007.3. Detección de objetos ausentes dentro de la unidad

- 007.4. Detección de movimientos e identificación de embarcaciones/objetos en la dársena.

- 007.5. Trazabilidad de vehículos dentro de Bases/Arsenales

ES_008: Del Sistema de centralización:

- 008.1. Integración y gestión inteligente de todos los sistemas en uno solo, con capacidad de generar presentaciones de distintos perfiles en función de la información que cada usuario de interés para cada usuario

- 008.2. Integración centralizada de alarmas mediante dispositivos IoT (Internet of Things).

- 008.3. Integración mediante dispositivos IoT de sistemas de iluminación de seguridad, con capacidad de monitorización y actuación.

- 008.4. Ayuda a la decisión respecto a las alarmas, para una óptima respuesta.

- 008.5. Detección de comportamientos anómalos del personal en función del historial.

ES_009: Del Sistema de simulación. El sistema tiene que tener la capacidad de generar distintos escenarios en todos los sistemas integrados que permitan evaluar de forma inteligente la eficacia y rendimiento de los operarios

ES_010: Sistema de comunicaciones seguras (enlace y conectividad):

- 010.1. Posibilidad de uso de redes 5G para la interconexión todos los dispositivos[3].

- 010.2. Creación de nube donde estén disponible todos los datos estructurados de los distintos sistemas y sensores, definiendo una ontología y semántica que garantice el acceso a los mismos

3 Actualmente la Armada tiene en proceso el proyecto Comunicaciones 5G en litoral / Base Naval.

ES_011: La arquitectura deberá responder a un esquema que verifique, al menos, los siguientes requisitos:

- 013.1.Gestión de eventos en tiempo real
- 013.2.Capacidad de crecimiento tanto en sensores como en elementos de gestión y clientes
- 013.3.Soportar cambio de tecnología en los sensores
- 013.3.Soportar cambio de tecnología en elementos de gestión
- 013.4. Protección contra fallos simples. Funcionamiento degradado
- 013.5. Soportar la desconexión entre cada AOR y que tengan funcionamiento independiente.

ES_012: La arquitectura global deberá corresponder a la combinación de los subsistemas básicos organizados en una estructura distribuida que permita el intercambio de información entre los diferentes nodos e interconectados todos ellos a la Plataforma como único sistema de nivel jerárquico superior y al resto de subsistemas de seguridad CCAA, CCTV, etc.

ES_13: El diseño debe permitir la optimización del ancho de banda de la red de comunicaciones y la velocidad de respuesta al consumir solo lo necesario para la transmisión de eventos.

ES_014: En modo normal de funcionamiento, la información transmitida consiste en eventos y metadatos si es aplicable.

ES_015: Los eventos del SCI deberán ser datados en origen y en tiempo real. Deberá existir una sincronización de los eventos con una resolución (no se exige precisión, pero si sincronización con el reloj del sistema, NTP) de milisegundos. Para el cumplimiento de este requisito, el licitador expondrá el mecanismo de gestión del reloj entre todos los dispositivos ofertado en su sistema.

ES_016: El licitador deberá describir con el mayor detalle posible cada módulo de su arquitectura propuesta, así como el flujo de información entre ellos.
ES_17: El licitador proporcionará un esquema de distribución del equipamiento que soporte la arquitectura ofertada, justificando su elección e indicando las funciones y capacidades de cada uno.
ES_018: El licitador deberá exponer, con todo detalle, los mecanismos de configuración y administración, tanto de manera remota como local.
ES_019: Se dispondrá de una interface de operación (IHM) con las siguientes características mínimas:

ES_019.1.La interfaz de usuario del sistema girará alrededor de una arquitectura de cliente ligero basado en arquitectura web, lo que aporta ventajas importantes:

- 019.1.1. No hay necesidad de distribuir software a los puestos de cliente.
- 019.1.2. El mantenimiento y las actualizaciones del sistema no suponen esfuerzo desde el punto de vista del despliegue, y se realiza para todos los usuarios a la vez.
- 019.1.3. Reducción de costes de gestión.
- 019.1.4. Configuración centralizada en los repositorios de configuración del propio sistema.

ES_019.2: El frontal web del sistema tendrá un diseño responsivo, es decir, se adapta a las capacidades del dispositivo y el navegador que utilizan los usuarios independientemente de la resolución de la pantalla en la que se utilice. Los navegadores probados para ser utilizados con el sistema serán:

- Edge (a partir de la v79).
- Firefox (a partir de la v68).

ES_019.3: La interfaz de usuario estará construida basándose en una arquitectura en dos capas que utiliza un frontal ligero. De acuerdo a esta arquitectura el sistema dispondrá de un conjunto de servicios que se ejecutan en un backend y que se encargan de entregar y recoger datos de la capa frontal, el frontend.

ES_019.4: El diseño funcional del frontal web del sistema girará alrededor de una estructura de navegación, que da acceso a las diferentes funcionalidades que ofrece el sistema, mediante una jerarquía con un máximo de tres niveles.

ES_020: Las características funcionales básicas que debe cumplir la plataforma son:

- 020.1. Funcionamiento orientado al seguimiento de los procesos de seguridad integrando datos de los sistemas y subsistemas existentes y capacidad de interoperabilidad con sistemas futuros. Utilización de estándares de interoperabilidad con seguridad intrínseca.
- 020.2. Capacidad de funcionamiento en modo seguro (redundante) y degradado con Back-ups automatizados.
- 020.3. Capacidad de georreferenciar toda la información.
- 020.4. Uso de cuadros sinópticos para el seguimiento de los procesos.
- 020.5. Uso de gráficos con indicadores de toda la actividad.
- 020.6. Generación sencilla de estadísticas e informes.
- 020.7. Correlación de la información y ayuda a la toma de decisiones. IA, Big-Data. Analytics, Casos de Uso, etc
- 020.8. Capacidad de integración con los sistemas existentes en las FAS.
- 020.9.Capacidad para publicar información de interés en la Intranet (avisos SEGFIS)

ES_021; La Interfaz hombre-máquina contendrá las siguientes características:

- 021.1. Amigabilidad: Deberán tener un diseño atractivo y una estructura clara de los contenidos que manejen.
- 021.2. Usabilidad: Su manejo deberá ser lógico, y permitir un acceso rápido a las funciones más utilizadas.
- 021.3. Navegabilidad: Deberá ser fácil navegar entre los contenidos, permitiendo conocer en todo momento el mapa de navegación, menú en que se encuentra el usuario y vuelta rápida al inicio. Se deberá poder acceder a cualquier elemento/pantalla en tres pasos o menos desde el menú principal.
- 021.4. Autoayuda: Deberá contar con funciones de autoayuda y manuales de uso.
- 021.5. Diseño Común: Todos los formatos de diseño serán comunes a todas las aplicaciones accedidas.
- 021.6. Interoperabilidad: Dispondrá de la capacidad de atender a dispositivos móviles.

- 021.7. Configurable: Deberá contar con herramientas de configuración que permitan al usuario elegir ciertas características particulares del interfaz, como el lenguaje utilizado, etc. Además, los interfaces de usuario se reconfigurarán para adaptarse al perfil del rol y usuario que acceda al puesto de trabajo.

ES_022: Fiabilidad. Para poder medir la calidad del sistema percibida por los operadores del mismo, se fijan unos parámetros porcentuales que establecen la porción de tiempo durante la cual están disponibles las funcionalidades consideradas bajo las condiciones de trabajo especificadas. De este modo, se pueden establecer valores de fiabilidad, mantenibilidad y disponibilidad del sistema.

ES_023: Para poder determinar la calidad del sistema desde el punto de vista de la fiabilidad y mantenibilidad, el licitador deberá proporcionar el MTBF y el MTTR respectivamente de su propuesta, indicando los métodos de cálculo utilizados para su obtención que garanticen la disponibilidad de la funcionalidad que prestan, o indicar los niveles de servicio comprometidos para el funcionamiento de la solución. En dicho cálculo se deberá considerar, al menos, los siguientes aspectos:

- ES_023.1.La arquitectura hardware y software de los sistemas y en especial:
- ES_023.2.Las configuraciones de alta disponibilidad.
- ES_023.3.La accesibilidad y modularidad de los componentes reemplazables.
- ES_023.4.La demostración fehaciente, mediante datos reales de fiabilidad mantenibilidad y disponibilidad, de la idoneidad de los elementos implantados en instalaciones reales con niveles de exigencia similar.
- ES_023.5.En los sistemas o módulos que no cuentan con redundancia, las paradas por razones de mantenimiento programado deberán ser tenidas en cuenta en el cómputo global de indisponibilidad del sistema.
- ES_023.6.En los sistemas o módulos con redundancia, se estimará la disminución de la fiabilidad debido a las paradas por razones de mantenimiento programado.

ES_024: Caso de resultar adjudicatario de los trabajos, los valores de fiabilidad, disponibilidad y mantenibilidad aportados por el licitador en su propuesta serán comprobados y exigidos sobre el sistema durante la fase de pruebas y garantía de la implantación.

ES_025: El trabajo del licitador no se dará como concluido hasta obtener unos resultados de fiabilidad, disponibilidad y mantenibilidad satisfactorios para La Armada y acordes a la propuesta inicial.

ES_026: Como mínimo se deberán garantizar los siguientes parámetros de disponibilidad para todos los elementos del sistema:

- 026.1: Tasa Máxima de Indisponibilidad de Servidores y Bases de Datos:3 hora al año.
- 026.2. Tasa Máxima de Indisponibilidad de Puestos de Operador: 12 horas al año.

ES_027: Adicionalmente a los estudios anteriormente referidos, el licitador expondrá el tiempo de vida útil estimada, la metodología de cálculo de la misma y el plan de cobertura de obsolescencia para valores menores de 10 años.

ES_028: Conforme a la Instrucción Técnica 01/14: Arquitectura Técnica Unificada del Ministerio de Defensa Versión 3.0 se hace una propuesta sobre lenguajes y tecnologías concretas. El licitador en su propuesta técnica puede aportar otra similar siempre y cuando las justifique y cumpla con las directrices establecidas por la Dirección Técnica:

Lenguajes, tecnologías y frameworks de desarrollo:

- JavaScript, JSON, XML, XSLT, SQL, XQL, jQuery, HTML/HTLM5, DHTML, CSS. AngularJS, JSP, JSTL, WSDL, WALD, React, CCS3, Material UI, Semantic UI.
- Java J2EE 1.8 y superiores.
- Framework java Spring Boot, Spring Webflow / MVC, Spring Security, Spring context /AOP, Spring Transaction, Spring Hibernate, Spring WS, JAXB, JAXWS, JAX-RS, Spring-REST, DisplayTag, jFreeChart.
- Framework MEDUSA MINISDEF
- BACKEND WEB: NodeJS con Express y WebSockets.
- BACKEND IA: Python, CUDA, Tensorflow, PyTorch +2.
- BACKEND DISTRIBUIDO: Golang, ProtoActor, Consul.
- Axis 1 o superior, CXF, Struts 1 o superior.
- Servicios web: SOAP, REST, cURL, WS-Security, WS-Interoperability.
- ORM: Hibernate.
- JDBC, PL/SQL
- Herramientas de reporting: Jasper Reports, Power BI, Tableau, Qlik, MicroStrategy.
- AUTENTICACIÓN INTRANET: LDAP, Active Directory, oauth2, Open, KEYCLOAK, SAMLv2.
- Firma electrónica PSSDEF: firma y Validación CAdES, XAdES, PAdES.
- Autenticación pública: Cl@ve, Autentic@SAMLv2
- CAS Server, SSO
- Aplicaciones móviles: Objective-C y Android. Flutter (Android y iOS).

- GIS y REMOTE SENSING: DeckGL, KeplerGL, OSM, CESIUM, QGIS, GDAL, RSGISLib, Geopandas, LiDAR, SciKit.

Sistemas operativos

- Linux/Unix: Red Hat 7 y superiores
- Windows: Windows Server 2012/2016, Windows 10.

Servidores web y de aplicaciones

- Apache 2 o superior.
- Servidores de aplicaciones: Oracle WebLogic 9.2 o superiores, 11g Server, Apache Tomcat 6.0.37 o superiores, JBOSS Server 5 o superiores
- DOCKER/SWARM
- KUBERNETES

Bases de datos

- Bases de datos relacionales: ORACLE 10g/11g/12c/19, PostgresSQL o equivalentes.
- Bases de datos documentales: Sistema de gestión documental EMC DOCUMENTUM (CMIS).
- BASES DE DATOS NOSQL: MongoDB
- BASES DE DATOS DE METRICAS: InfluxDB, ElasticSearch
- PORTAL DOCUMENTAL: CKAN

ES_029: El adjudicatario se compromete a utilizar en sus trabajos la plataforma de desarrollo proporcionada por el Ministerio de Defensa, tanto en cuanto a repositorio de código y herramientas, como a repositorios de documentación y a adaptarse a las normas de uso de dicho entorno proporcionadas por el Ministerio de Defensa. Las herramientas disponibles en este entorno en el momento de escribir este pliego son:

- Sistema de control de versiones: GitLab, Subversion.
- Sistema de generación automática: Jenkins, GitLab Pipelines.
- Sistema de control de calidad: SonarQube.
- Sistema de gestión de logs: RSysLog, ElasticSearch.
- Herramientas ofimáticas: MS/OFFICE. LibreOffice.

- Repositorio de artefactos: Nexus, Docker Hub.
- Herramienta de modelado: ERWin Data Modeler, Enterprise Architect, Bizagi Modeler, ARIS.
- Herramientas integradas de desarrollo: Eclipse, Visual Studio, maven, Eslint.
- Herramientas de ticketing: SCANS, RTC, JIRA, Mantis.
- Herramientas colaborativas: Sharepoint.

Gestión de proyectos

- Planificación de proyectos: OpenProject, Trello y MS-Project.
- Sistema de gestión de pruebas: TestLink.
- Otros productos de pruebas y evaluación
- JUnit, NUnit, DBUnit, PHPUnit.
- SoapUI.
- Mockito y HarmCrest.
- Jmeter.
- Selenium.
- Swagger, Postman.

ES_030: Funcionamiento autónomo: Cada uno de los subsistemas deberá poder funcionar de manera autónoma sin necesidad de la plataforma.

ES_031: Todos los subsistemas deberán disponer capacidad para integrase en la plataforma y para ello deberán disponer de interfaces de comunicación IP, y protocolos de integración, como SNMP, MODBUS-TCP, MQTT o similar, no propietario, o de un interfaz de tipo API REST. Dichos mecanismos de integración deberán permitir la monitorización del estado de los subsistemas (telemetría), y la operación de los mismos (envío de comandos).

ES_032: Del Sistema de control: Arquitectura cliente-servidor.
• Software ABIERTO y multisite compatible con múltiples fabricantes de cámaras analógicas e IP.

En el caso de que se realicen nuevas instalaciones de cableado serán de aplicación los siguientes requisitos:

•ES_033: Cableado de fibra óptica o cobre según requisitos de sensores, ubicación y distancias.

●ES_034: Cableado UTP cat. 6A entre los Switchs y los dispositivos CCTV (tanto Cámaras como grabadores).

● ES_035: Elementos auxiliares de conexión como pigtails, enfrentadores, bandejas de parcheo…

● ES_036: Cajas estancas IP66 400x300x200 mm en cada uno de los 5 Emplazamientos.

4.2.DE SEGURIDAD

Se determinan los siguientes requisitos de seguridad:

RS_001: La empresa adjudicataria deberá adoptar las medidas necesarias para garantizar la interoperabilidad de los sistemas en el contexto de la AGE. En concreto, los sistemas deberán cumplir las medidas establecidas en el Esquema Nacional de Interoperabilidad que sean de aplicación en los productos y servicios suministrados.

RS_002: La empresa adjudicataria se compromete a cumplir todo lo especificado en materia de seguridad de la información por la normativa vigente en el Ministerio de Defensa y en especial lo especificado en la "Política de seguridad de la información del Ministerio de Defensa" (OM 76/2006, de 18 de abril) y todas aquellas normas de rango inferior que emanan de esta política

RS_003: El adjudicatario se atendrá a la normativa y recomendaciones más actuales del CCN-CERT relativas a tecnologías y dispositivos que sean de aplicación a las soluciones y sistemas objeto de la presente licitación.

RS_004: El adjudicatario quedará obligado a configurar de forma segura todos los dispositivos y sistemas objeto del contrato, en particular:

- Los sistemas se configurarán de manera que garanticen la seguridad por defecto, conforme a lo establecido al respecto en el artículo 19 del ENS, en particular los sistemas proporcionarán la mínima funcionalidad requerida para alcanzar los objetivos fijados, las funciones de operación y administración serán las mínimas necesarias y su uso será sencillo y seguro, de forma que una operación insegura requiera de un acto consciente por parte del usuario.

- Deberán cambiarse las credenciales por defecto de cualquier dispositivo que tenga conectividad de red IP y disponga de un mecanismo de autenticación electrónica para acceder a algún tipo de funcionalidad restringida.

- Cualquier dispositivo o sistema que se suministre como parte de este contrato, que tenga conectividad de red IP y disponga de la funcionalidad de administración remota, deberá soportar la conexión a través de un canal cifrado de tal forma que los datos de autenticación no viajen en claro.

- Cualquier ordenador personal, portátil o servidor, que se suministre como parte de este contrato, deberá contar con un chip criptográfico TPM 2.0 que le permita custodiar el material criptográfico de manera segura. En caso de que no se pueda

cumplir este requisito, se deberá justificar detalladamente las razones y esta excepción deberá ser autorizada previamente por el Ministerio de Defensa.

- Cualquier ordenador personal, portátil o servidor, que se suministre como parte de este contrato, deberá de soportar los siguientes estándares: "Unified Extensible Firmware Interface (UEFI)" con tablas de particiones GPT. En caso de que no se pueda cumplir este requisito, se deberá justificar detalladamente las razones y esta excepción deberá ser autorizada previamente por el Ministerio de Defensa.

- Cualquier dispositivo de red que se suministre como parte de este contrato, deberá de soportar los siguientes estándares: IEEE 802.1X. En caso de que no se pueda cumplir este requisito, se deberá justificar detalladamente las razones y esta excepción deberá ser autorizada previamente por el Ministerio de Defensa.

- El adjudicatario realizará un seguimiento de las vulnerabilidades que se descubran sobre los dispositivos y sistemas objeto del presente pliego y dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.

RS_005: Todos los interfaces de administración de sistemas y equipamientos hardware deberán poder ser configurados para utilizar protocolos seguros. Las interfaces de administración en ningún caso estarán protegidas por certificados que no sean susceptibles de ser sustituidos por uno propio del Ministerio de Defensa. El adjudicatario se atendrá a lo indicado en la guía de buenas prácticas CCN-CERT BP-01/17 para la implementación de HTTPS en todos aquellos sistemas y aplicaciones del nodo donde dichas recomendaciones sean de aplicación.

RS_006: El adjudicatario realizará un Análisis de Riesgos para cada uno de los servicios, de acuerdo con la metodología establecida en el Esquema Nacional de Seguridad, identificando los activos que intervienen en la prestación del servicio, las amenazas, las salvaguardas presentes, su nivel de madurez, la probabilidad de que las amenazas se materialicen, el posible impacto en el servicio y las acciones a tomar para reducir el riesgo a un nivel aceptable para el responsable del servicio.

RS_007: Se permitirá hacer uso de protocolos seguros de comunicaciones, como por ejemplo SSL, TLS, SSH, HTTPS, S/MIME, etc. En aquellos servicios que sea posible, se finalizarán las conexiones seguras en elementos de seguridad intermedios, de modo que se permita la inspección y auditoría de la información "en claro", para detectar y prevenir amenazas.

RS_008: Las soluciones técnicas a implementar deberán garantizar su adecuada interoperabilidad con el resto de sistemas integrados en la I3D con base al cumplimiento de los estándares del Catálogo de Estándares del ENI y en el Catálogo Unificado de Estándares del Ministerio de Defensa.

RS_009: Los productos ofertados (hardware, software, firmware, etc.) relacionados directa o indirectamente con la transmisión, manipulación o procesamiento de información por medio del protocolo IP deben ser capaces de operar plenamente de acuerdo a los estándares comerciales establecidos para el protocolo "IPv6" y a los aspectos definidos en el RFC 2460 (Internet Protocol Version 6 Specification) y el resto de RFC relacionados con "IPv6".

RS_010: Los locales donde se alojen el CRAU y los CRA correspondientes estarán en disposición de ser acreditados con el nivel de Zona de Acceso Restringido (ZAR).

RS_011: Se procurará que todos los sistemas de seguridad instalados que requieran de suministro eléctrico para su funcionamiento estén conectados a un circuito eléctrico exclusivo destinado a seguridad, que disponga de un grupo electrógeno automático y de los sistemas de alimentación ininterrumpida (SAI) necesarios para garantizar su funcionamiento y preservar los equipos frente a caídas y/o picos de tensión y/o cortes en el suministro.

RS_012: El cableado utilizado deberá cumplir los siguientes requisitos:

• 012.1:Los cables utilizados serán libres de halógenos (UNE-EN 50267-2-1 o equivalente) no propagadores de llama (UNE-EN 60332-1-2 o equivalente, UNE-EN 60332-3-24 o equivalente), de reducida emisión de gases tóxicos (NFC 20454), de baja emisión de humos opacos (UNE-EN 61034-2 o equivalente), nula emisión de gases corrosivos (UNE-EN 50267-2-2 o equivalente) y estarán clasificados con una clase mínima de "Cca-s1b, d1, a1" según el Reglamento de productos para la construcción (CPR) de la Unión Europea.

• 012.2: Se utilizará cable de tres conductores o dos según normativa, conectando la masa, si procediera, en ambos extremos de la tirada, incorporando las protecciones eléctricas que sean necesarias, y garantizando el cumplimiento de la normativa aplicable.

• 012.3: El adjudicatario será el encargado de realizar toda la instalación, aportando todos los medios materiales necesarios, para realizar la conexión a la red.

5. REQUISITOS DE LOS TRABAJOS DEL CONTRATISTA

5.1. DE INSTALACIÓN

Se determinan los siguientes requisitos:

RTCI_001: En caso de que los trabajos de apoyo a la instalación del sistema necesiten un proyecto de obras, la empresa adjudicataria presentara el correspondiente proyecto de obras, que será supervisado por la Jefatura de Infraestructura del Arsenal/JESAT, o cuando corresponda por el Área de Supervisión de Proyecto de la DIN. La Armada podrá colaborar con la empresa para la realización del proyecto.

RTCI_002: El contratista dispondrá de un entorno de implementación, actualización y pruebas del sistema en la Oficina Técnica de Supervisión y Operación para la realización de pruebas y estudios.

RTCI_003: El Adjudicatario se compromete a realizar la actividad, objeto del Pliego, con personal cualificado para tal fin.

RTCI_004: El contratista se comprometerá a guardar absoluta confidencialidad sobre todas las tareas, actividades y conocimientos que se deriven de la ejecución de este proyecto siendo de obligado cumplimiento lo contenido en el artículo 133 de la ley.

9/2017, de 8 de noviembre, de Contratos del Sector Público.

Todos los documentos que se generen tienen carácter confidencial y no podrán ser total ni parcialmente reproducidos en ningún medio, o entregados a terceras personas.

Para la obtención de los objetivos marcados en este PPT es necesaria la creación de equipos de trabajo multidisciplinares, que soporten todas las actividades y etapas del proyecto. Los distintos equipos de trabajo deberán actuar de manera coordinada con el fin de cumplir con la planificación y tareas previstas. Los equipos de trabajo pueden ser unipersonales o no en función de la dedicación de sus componentes y de los objetivos funcionales del grupo.
El licitador deberá incluir en su propuesta al menos la siguiente información:

- Número y denominación de los equipos de trabajo que llevarán a cabo el proyecto.
- Número de personas y nombre de cada una de ellas que constituirán cada grupo de trabajo (al menos de los responsables del mismo).
- Experiencia de los miembros de los equipos de trabajo.
- Formación de los miembros de los equipos de trabajo.
- Funciones asignadas a cada uno de los miembros del equipo de trabajo.
- Dedicación al presente expediente de cada uno de los miembros de los diferentes equipos de trabajo.

El número mínimo de grupos de trabajo identificados serán los siguientes:
Director de Proyecto: Titulado Universitario con al menos 10 años de experiencia demostrable en la Gestión de Grandes Proyectos. Podrá apoyarse en un equipo de expertos con el fin de cumplir el PAC. Serán obligación del Director del Proyecto las siguientes actividades o acciones:

- Deberá tener disponibilidad inmediata en caso de ser reclamado por la Armada, sin ser posible ningún tipo de condicionante que lo pudiera redimir de dicha acción.
- Será el Interlocutor entre el Adjudicatario y la parte de Armada de la Oficina Técnica de Supervisión y Operación pudiéndose apoyar en cualquiera de sus especialistas (Director Técnico del Proyecto, responsable del equipo de diseño, etc.).
- Deberá iniciar y coordinar las tareas con los usuarios de la Armada, y otros facultativos afectados por la instalación.
- Deberá proporcionar día a día la supervisión del personal contratado o subcontratado, así como velar por el cumplimiento de todas las normas de seguridad impuestas por las normas vigentes que sean de aplicación.
- Deberá coordinar y controlar a todos y cada uno de los miembros de su equipo.
- Deberá asegurar el cumplimiento de lo acordado con la Oficina Técnica de Supervisión y Operación por parte de La Armada en cuanto al alcance del Proyecto de Ejecución y sus revisiones.

- Será el único responsable del cumplimiento de los plazos fijados para la ejecución de las tareas.
- Elaborará y presentará informes de seguimiento del avance del proyecto.
- Será responsable de la documentación a entregar.
- Deberá realizar la gestión de la calidad del proyecto.
- Será el máximo responsable ante situaciones indeseadas provocadas por el Adjudicatario.

Deberá tener un perfil orientado a:

- Relación con los usuarios para toma de requisitos funcionales y técnicos.
- Análisis de sistemas de información.
- Proyectos con aplicación de la metodología aplicada al presente proyecto.
- Uso de herramientas para especificación de requisitos y análisis del Sistema.
- Aplicación de técnicas y herramientas para el control y gestión de configuración acordes con la metodología aplicada al presente proyecto.

Director Técnico: Titulado Universitario con al menos 5 años de experiencia demostrable en Sistemas de Seguridad. Serán obligación del Director Técnico las siguientes actividades o acciones:

- Deberá tener disponibilidad inmediata en caso de ser reclamado por La Armada, sin ser posible ningún tipo de condicionante que lo pudiera redimir de dicha acción.
- Será el Interlocutor entre el Adjudicatario y la Dirección Técnica por parte de La Armada en los asuntos relacionados con la operativa y la funcionalidad de la plataforma (análisis del sistema).
- Será su obligación entender las necesidades operativas y funcionales de todos y cada uno de los usuarios del sistema. Para ello mantendrá todas las reuniones estime oportunas bajo la supervisión y coordinación de la Dirección Técnica de La Armada.
- Será responsable de satisfacer las necesidades operativas y funcionales de todos y cada uno de los usuarios del sistema.
- Será responsable de entender los procedimientos a implantar en el sistema.
- Será responsable de perfeccionar los procedimientos existentes, con objeto de satisfacer todas las necesidades operativas y funcionales de todos y cada uno de los usuarios del sistema.
- Elaborará y presentará la documentación resultante de las acciones anteriores.

Equipo de Diseño: Equipo de Trabajo encargado de garantizar la realización de las actividades necesarias para la obtención de las soluciones adecuadas a los requerimientos planteados en el presente PPT. Estará constituido por personal con experiencia demostrable en diseño y dirección de la implantación de plataformas similares al recogido en el presente PPT. Podrá estar constituido por distintos profesionales en función de la especialidad concreta del expediente de la que se hacen responsables. Será obligación del Equipo de Diseño las siguientes actividades o acciones:

- Deberá tener disponibilidad inmediata en caso de ser reclamado por Armada, sin ser posible ningún tipo de condicionante que lo pudiera redimir de dicha acción.

- Será el Interlocutor entre el Adjudicatario y la Oficina Técnica de Supervisión y Operación por parte de la Armada en los asuntos relacionados con el diseño del sistema.
- Será el responsable del diseño físico y lógico del sistema.
- Será el responsable de la implantación del equipamiento HW y SW.
- Será responsable ante situaciones de error en el diseño o la implantación del sistema.
- Deberá asumir las indicaciones del Director Técnico con el fin de satisfacer las necesidades funcionales y operativas del sistema.

Deberá contar con perfiles con experiencia en:

- Proyectos de integración de sistemas de seguridad industrial.
- Interconexión de sistemas, comunicaciones basadas en normativas y estándares de mercado.
- Gestión de procesos de usuarios.

Equipo de Instalación y Pruebas: Equipo de trabajo encargado de comprobar la implantación del sistema en el CPI y en producción. Deberá estar constituido por personal con experiencia demostrable en trabajos similares. Entre sus principales actividades se encuentra:

- Garantizar la instalación del sistema en el entorno de pruebas.
- Garantizar la instalación del sistema en producción.
- Asistir y coordinar las pruebas operativas.
- Realizar el apoyo a la transición.
- Llevar a cabo la formación operativa de los usuarios.
- Coordinarse con el Director Técnico de modo que se asegure que se alcanzan los objetivos propuestos para el sistema.

Equipo Programador: Grupo de trabajo encargado de traducir el diseño de los sistemas SW en instrucciones que formen parte de un aplicativo. Estará constituido por personal con experiencia demostrable en trabajos similares. Será obligación del Equipo de Diseño, entre otras, las siguientes actividades o acciones:

- Generación del Código Fuente y Código Objeto.
- Creación de las bases de datos.
- Compilar los programas desarrollados y obtener el Código Ejecutable.
- Realizar la depuración del sistema.
- Adaptación e integración de los distintos sistemas entre sí.
- Captura y envío de información con equipos o sistemas externos.
- Deberá asumir las indicaciones del Equipo de Diseño para alcanzar los objetivos plateados por éste.

Deberá contar con perfiles con experiencia en la parametrización y programación en entorno de herramientas de cada uno de los módulos que forman parte del sistema:

- Interfaces IHM.
- Indicadores
- Cuadros de mando.
- Gestión de procesos
- Gestión documental
- BBDD
- Integración de sistemas.
- Etc.

Oficiales de Instalación: Certificados y aprobados por el fabricante de los equipos a instalar con experiencia demostrable de al menos 2 años en la instalación de equipos de similares características a los incluidos en el presente PPT. Se podrá contar con tantos oficiales de instalación como bloques funcionales estén incluidos en el alcance del proyecto.

Equipo Responsable de la Seguridad y Salud Laboral: Adicionalmente al personal técnico asignado al proyecto, el Adjudicatario incluirá obligatoriamente en su organigrama el siguiente personal como responsable de seguridad y salud en la ejecución del proyecto:

Coordinador en materia de seguridad y salud durante la elaboración del proyecto de instalaciones. Técnico competente del Adjudicatario, que previa aprobación y nombramiento por parte de la Armada, desarrollará las funciones definidas en el R.D. 1627/1997, de 24 de Octubre, durante la elaboración del proyecto de instalaciones.

Coordinador en materia de seguridad y salud durante la ejecución del proyecto. Técnico competente designado y aportado por el Adjudicatario, que previa aprobación y nombramiento por parte de la Armada, desarrollará las funciones definidas en el R.D. 1627/1997, de 24 de Octubre, durante la ejecución de la Instalación.

La no inclusión de los datos referidos al organigrama y requeridos en las propuestas de las empresas licitadoras, puede ser causa suficiente para la no valoración de las mismas y exclusión automática.

Se deberá indicar en las propuestas la estimación de horas que dedicará cada uno de los miembros principales del equipo de trabajo al desarrollo de los mismos. Dicha estimación será meramente informativa, sin ser en ningún modo restrictivo ni vinculante al desarrollo posterior de los trabajos. El adjudicatario deberá dedicar el tiempo necesario al desarrollo de los trabajos hasta alcanzar los objetivos perseguidos, sin obtener ningún tipo de compensación económica adicional en caso de necesidad de aumentar el equipo o las horas de trabajo previstas.

Cualquier componente del personal dedicado por el adjudicatario al proyecto puede formar parte del grupo de expertos sin resultar necesaria la incorporación de ningún técnico adicional siempre que cumpla los requisitos, en cuanto a la cualificación otorgada por el fabricante, mencionados.

La facultad de control, dirección del trabajo y de los trabajadores corresponde a la empresa adjudicataria por disponer la misma de una titularidad independiente a la Armada, así como de organización autónoma.

En el supuesto de que se produzcan quejas motivadas contra trabajadores, por falta de capacidad o incorrecto comportamiento, la Armada dará traslado de las mismas, a través de la Oficina del Proyecto, estando obligado el Adjudicatario a la sustitución de dicho personal.

El personal, al servicio del Adjudicatario, adscrito a la actividad objeto de este Pliego, una vez finalizada ésta o si la misma se resolviera antes de finalizar la vigencia pactada, seguirá perteneciendo a la plantilla del Adjudicatario, siendo la Armada totalmente ajena a las relaciones laborales entre el Adjudicatario y sus empleados, así como a las responsabilidades que de tales relaciones laborales pudieran derivarse, por no darse el supuesto de subrogación empresarial.

5.2. DE VERIFICACION, CALIDAD, VALIDACION Y PRUEBAS

Se determinan los siguientes requisitos:
RTCV_001: Sera de aplicación, para el desarrollo del presente contrato, la normativa de calidad que se recoge en la Publicación Española de la Calidad, PECAL 2110 o AQAP equivalente.
El material o servicio objeto del presente contrato no podrá ser recibido hasta que se otorgue al contratista un certificado de conformidad de calidad por la Dirección General de Armamento y Material o por la autoridad u organismo en quién el Director General de Armamento y Material haya designado las funciones de inspección y calidad.
RTCV_002: El adjudicatario, una vez adjudicado el contrato y antes de la fecha programada para el inicio de los trabajos, enviará al responsable del Contrato un Plan de Aseguramiento de Calidad. Se evaluará y comunicará por escrito al adjudicatario su aprobación o los comentarios que crea oportunos. El adjudicatario estará obligado a atender a dichas observaciones que se pudiera hacer antes del inicio de los trabajos.
Además de aquellos aspectos comunes a todas las fases que pueda contemplar el PAC inicial entregado por el contratista, el adjudicatario deberá elaborar un PAC distinto y específico para cada actividad o fase del proyecto, pudiendo ser entregado y aprobado o comentado de forma paulatina conforme avance la implantación del sistema. El Plan de Calidad, tanto el general como los correspondientes planes específicos, incluirán como mínimo, la descripción de los siguientes conceptos cuando sean aplicables:

- Organización.
- Procedimientos, instrucciones y estándares a aplicar.
- Productos a revisar.
- Control de materiales y servicios contratados.
- Manejo, almacenamiento y transporte.
- Procesos especiales.
- Inspección de implantación por parte del Contratista.
- Gestión de la documentación.

Si en la organización del oferente ya existe un sistema de calidad, el PAC deberá ser coherente con el mismo, completándolo en los aspectos relativos a normas particulares relacionadas con este Contrato.
Si no existe, se basará en los estándares:

- UNE-EN-ISO 9001:2008 Sistemas de Gestión de la Calidad – Requisitos.
- UNE-EN-ISO-14001:2004 Sistema de Gestión Medioambiental.

RTCV_003: Los costes ocasionados al Adjudicatario como consecuencia de las obligaciones que contrae en cumplimiento del PAC y del Pliego de Prescripciones, serán de su cuenta y se entienden incluidos en los precios de proyecto.
Por consiguiente, serán también de cuenta del adjudicatario, tanto los ensayos y pruebas que éste realice como parte de su propio control interno de calidad, como los establecidos por La Armada para el control formal de calidad que permita la "recepción" de los sistemas y que están definidos en el presente Pliego de Prescripciones Técnicas o en la normativa general que sea de aplicación al presente proyecto.

El Adjudicatario suministrará, a su costa, todos los materiales que hayan de ser ensayados, así como el equipamiento y personal necesario para ello.

5.3. DE APOYO LOGISTICO INTEGRADO/CICLO DE VIDA

Se determinan los siguientes requisitos:
RTCA_001: El objetivo del Control de la Configuración es asegurar que el material objeto del contrato queda definido funcional y físicamente por los planos, dibujos, especificaciones y cualquier otra documentación relacionada con las mismas. El Control de la Configuración se aplicará a todos los elementos del sistema, sus componentes físicas y lógicos (software), los equipos de apoyo, las instalaciones y la documentación.
RTCA_002: Para el Control de la Configuración se adoptará metodología ISO 12207 o equivalente para el ciclo de vida del desarrollo. A tal efecto, el adjudicatario establecerá una Configuración de Referencia.

5.4. REQUISITOS DE FORMACIÓN

Se determinan los siguientes requisitos:
RTCF_001: El adjudicatario deberá elaborar un plan de formación en el uso y mantenimiento para personal de la Armada con su documentación correspondiente orientada en 2 grandes modalidades:

- Formación Técnica: Orientada al mantenimiento y explotación de los equipos de campo y sistemas implantados.
- Formación Operativa: Orientada a la operación y gestión de la plataforma con objeto de sacarle el máximo rendimiento a todas sus capacidades.

RTCF_002: El sistema deberá contar con un módulo de simulación en cada AOR para adiestramiento del personal.

5.5. REQUISITOS DE DOCUMENTACIÓN

Se determinan los siguientes requisitos:
RTCD_0001: El adjudicatario deberá presentar un calendario de entrega de la documentación, en concordancia con los hitos parciales del programa, que será aprobado por la Oficina Técnica de Supervisión y Operación.
RTCD_0002: La lista de documentación a entregar por el contratista durante el desarrollo de los trabajos enumera la documentación mínima que éste deberá presentar a La Armada, compuesta por:

1. Plan General del Proyecto.
2. Plan de Garantía de Calidad.
3. Plan de Control de Configuración.
4. Plan de Gestión de Documentación.
5. Plan de Seguridad y Salud.
6. Plan de Pruebas y Protocolos de Pruebas.
7. Plan de Instalación.
8. Plan de Formación.
9. Plan de Mantenimiento.

10. Plan de seguridad informática.
11. Plan de explotación.
12. Estudio previo instalación de elementos de campo.
13. Diseño de la Instalación. Deberá proporcionar información con:
    - Memoria descriptiva de la instalación.
    - Planos detallados de todas las instalaciones realizadas, que permitan la identificación individual con el grado de detalle descrito en el PPT o en actas realizadas. Se entregarán por parte del contratista en soporte papel en formato a determinar y en soporte electrónico para su posterior mantenimiento.
    - Diagramas de conexión.
    - Planos de los Racks.
    - Plan de direccionamiento IP
    - Ficheros de configuración de los equipos/Sensores
    - Etc.
14. Descripción del Equipamiento. Comprenderá la descripción de todos y cada uno de los:
    - Sistemas/Equipos y unidades integrantes del suministro. Inventario de equipos.
    - Instrumentos de prueba y herramientas especiales.
    - Arquitectura del Sistema/Equipo.
    - Diagrama de conexión interno y externo.
    - Albaranes de entrega de equipos debidamente cumplimentados y firmados.
    - Lista de comprobación de recepción de equipos con el grado de detalle necesario: modelo, cantidad, versión, números de serie, licencias software, etc. En la lista de comprobación se detallan las discrepancias y no conformidades que se observan en relación a los equipos y elementos previstos.
15. Informes de Resultados de Pruebas de Instalación. Informe de pruebas del sistema. Se adjuntará la relación de pruebas que se han realizado para cada uno de los equipos o elementos que garantiza su funcionamiento individual. Se aportará documento que acredita que las pruebas se han pasado de forma satisfactoria con la relación de discrepancias y en su caso de no conformidades declaradas. Se aportarán los certificados, y homologaciones oficiales para su adecuación respecto a la normativa y estándares correspondientes. Esta documentación se realizará para cada una de las fases de pruebas que se establezcan.
16. Informes de Inspección de Instalación de Equipos.
17. Informe de Pruebas de Aceptación.
18. Manuales Técnicos de Administración.
19. Manual de Usuario. El adjudicatario debe redactar el manual de usuario específico para el sistema implementado que contemple todas las funciones programadas y acciones a realizar.
20. Manual de Mantenimiento y Operación del Sistema y Equipos. De igual forma que el manual de usuario, se deberán redactar los manuales de Mantenimiento y Operación del Sistema y Equipos a medida para la implantación realizada. El adjudicatario está obligado a redactar dichos manuales contemplando el sistema como una integración de subsistemas y equipamiento. No se permitirá la entrega

única de una recopilación de manuales de Mantenimiento y Operación de equipos o sistemas.
21. Documento de especificaciones.
22. Documentos de análisis y diseño. En este capítulo se incluye toda la documentación realizada durante las etapas de análisis y diseño del sistema, incluido el documento de "Arquitectura del Sistema".
Toda la documentación entregada, deberá estar revisada por el responsable de calidad y aprobada por el director del expediente.
El adjudicatario deberá entregar los manuales y documentos del fabricante que acompañan a cada equipo, necesarios para la explotación del hardware, así como uso y mantenimiento del software de base a adquirir en este expediente.

REQUISITOS DE CERTIFICACION

Se determinan los siguientes requisitos:
RTCC_001: La empresa adjudicataria deberá estar en posesión de los siguientes certificados:

- Certificación ISO 9000.
- Certificación ISO 20000-1.
- Certificación ISO 27001.
- Certificado de Conformidad con el Esquema Nacional de Seguridad.

RTCC_002: Una vez finalizada la instalación y antes de la recepción provisional se comprobará el buen funcionamiento de toda la instalación, verificando su correcto funcionamiento.

RTCC_002.1: La empresa instaladora dispondrá del personal e instrumental técnico y materiales necesarios para realizar una revisión general de toda la instalación y la Dirección Facultativa emitirá la Certificación Final de la instalación, cuando la instalación este totalmente finalizada y funcionando correctamente según lo previsto en el proyecto de ejecución.

RTCC_002.2: Para realizar la certificación se utilizará un equipamiento de medida adecuado a cada tipo de instalación, con certificado de calibración en vigor, una copia del cual deberá aportarse junto con el informe de certificación.

RTCC_002.3: Cada medida se almacenará con un identificador único, que permita su fácil localización.

RTCC_003.: La red eléctrica debe cumplir el Reglamento Electrotécnico de Baja Tensión. La empresa instaladora debe elaborar los boletines necesarios y realizar los trámites de aceptación de la instalación eléctrica ante los organismos competentes.

RTCC_004: Dentro del control de calidad, se han de llevar a cabo pruebas de calidad del tendido realizado y de continuidad con la red existente del 100% de las secciones, empalmes y conectores, en todos los tramos afectados por el tendido.

RTCC_005: Las pruebas que se deberán realizar para la validación y aceptación de los trabajos de instalación del cable de fibra óptica serán de diversos tipos:

•005.1: Mediciones de atenuación.

•005.2: Visuales.

• 005.3: Otras pruebas de calidad.

RTCC_006: Las mediciones se realizarán en el 100% de las secciones y empalmes afectados por el tendido.

RTCC_007: Comprobaciones visuales para el cable:

• 007.1: Verificación de que hay cable instalado.

• 007.2: Verificación de que el cable se ha tendido por el conducto designado para ello.

• 007.3: Verificación del correcto etiquetado del cable.

• 007.4: Verificación de que el radio de curvatura del cable es superior al especificado en todas las arquetas del recorrido.

RTCC_008: Comprobaciones visuales para la caja de empalme:

• 008.1: Correcto estado de la caja de empalmes.

• 008.2: Correcta instalación de la misma.

• 008.3: Correcta protección y ubicación de los empalmes en la caja.

• 008.4: Correcto corte de los cables para realizar el empalme.

• 008.5: Correcta etiquetación de los empalmes y durabilidad de la misma.

• 008.6: Correcto cierre y ubicación de la caja en la arqueta.

• 008.7: No deterioro de la caja en su apertura, manipulación o cierre.

• 008.8: Eliminación de escombros y sobrantes.

RTCC_009: Comprobaciones visuales para el repartidor óptico (en caso de tener):

• 009.1: Correcto estado del repartidor óptico.

• 009.2: Correcta instalación del mismo.

• 009.3: Correcta limpieza de los conectores.

• 009.4: Correcta realización de la conectorización.

• 009.5: Limpieza y recogida exhaustiva de los materiales sobrantes y escombros producidos en la ejecución.

REQUISITOS DE LOS ELEMENTOS A SUMINISTRAR

Presentación de la documentación:

1. Todos los documentos deberán estar escritos en idioma castellano. Excepcionalmente y previa autorización de la Armada será admitida documentación técnica o catálogo de productos en inglés.
2. Para cualquier documento del proyecto, el Contratista deberá fijar el tipo y tamaño de letra, interlineado, márgenes, cabeceras, pies, presentación de títulos de apartados y cualquier parámetro que defina el estilo de los documentos, que deberá ser aprobado por La Armada.
3. Todo documento, deberá contener:

Una portada común para todo el proyecto, conteniendo:

- Proyecto.
- Título.
- Nº de Documento.
- Código.
- Fecha de edición.
- Logotipo de La Armada.

Hoja de control, que contendrá la siguiente información:

- Una tabla que indicará, para cada edición, las revisiones que tiene, fecha, páginas afectadas y razones de los cambios
- Una tabla que contendrá, para cada página del documento, la edición y revisión.

4. Toda página de un documento deberá tener como mínimo: código, fecha, nº de página, cambio que la afecta, proyecto y título.
5. Las páginas que no conformen el cuerpo del documento, deberán numerarse con números romanos en mayúscula. El cuerpo del documento, en números arábigos relativos a cada capítulo o anexo.
6. El índice deberá contener los números en que comienzan los diferentes capítulos del documento, con una línea de puntos desde el final del título del apartado al número de página.
7. Todo documento, deberá contener un capítulo inicial con el siguiente contenido:

- Objeto: que deberá describir el objeto del documento.
- Alcance: que indicará el ámbito de aplicación del documento.
- Identificación: deberá identificar de forma precisa el sistema y el proyecto a que se aplica el documento, así como la finalidad y objetivos de los mismos.
- Estructura del documento: describirá la organización y las partes fundamentales del mismo.
- Documentación de referencia: identificará otros documentos a los que se haga referencia desde éste, agrupándolos por tipos (normas, etc.), especificando para cada uno de ellos el título, código y versión.
- Definiciones: deberá contener las definiciones necesarias para la comprensión del documento.

- Siglas y abreviaturas: deberá contener todas las siglas, abreviaturas y acrónimos que se encuentren a lo largo del texto, tablas y dibujos del documento.

8. La documentación deberá editarse con los programas de Microsoft-Office, y formato DWG y PDF para planos, debiendo estar integrados en un solo documento tanto el texto como figuras, calendarios, etc. Se utilizará la versión de los programas que corresponda y que sea autorizada por la Armada
9. Todos los documentos deberán ir encuadernados usando carpetas blancas de 2/4 anillas o fastener. Las portadas, en ambos casos, podrán ser de colores en función del tipo de documento, y en la lomera de la carpeta figurará al menos el título del documento y nombre del proyecto.
10. En todos los documentos deberá figurar el logotipo de la Armada, pero nunca el del Contratista, el cual sólo deberá aparecer como autor del mismo.
11. Para las hojas de los documentos, se deberá utilizar el formato DIN A4, pudiéndose utilizar DIN A3 si el tamaño de dibujos o tablas así lo justificaran.
12. Todo documento deberá tener un código único que lo identifique unívocamente, el cual contendrá información relativa a:
    - Originador.
    - Subsistema.
    - Nº de orden.
    - Tipo de documento (manual, especificación, etc.).
    - Versión.
    - Provisionalidad.
13. Siempre debe entregarse un documento completo tanto en papel como en soporte informático. Sólo cuando esto no sea posible, de forma justificada, se admitirá que se envíe un documento en varias entregas, y en este caso el Contratista deberá suministrar el índice completo con la primera entrega.
14. Cuando un documento no cumpla con los requisitos de documentación, deberá ser modificado por el Contratista tantas veces como sea necesario hasta que cumpla con dichos requisitos.
15. Cuando el contenido de un documento sufra cambios en conceptos, estrategias o elementos básicos, el Contratista deberá generar una nueva versión.
16. Todo cambio a un documento, se deberá realizar siguiendo los procedimientos establecidos para ello y aprobados por la Armada.
17. Los documentos (tanto las copias en papel como en soporte informático) se entregarán formalmente al responsable de la Armada de la Oficina Técnica de Supervisión y Operación.
18. Se realizará un listado que habrá de mantenerse actualizado incluyendo toda la documentación aportada por el adjudicatario.

Como norma general, el Contratista deberá entregar 1 copia de cada documento tanto en papel como en soporte informático, ya sea borrador, primera o última versión, para su evaluación y validación. Una vez validado el documento, La Armada podrá exigir una copia adicional que deberá ser entregada como máximo en los 10 días siguientes a la petición del documento.

6. CALIDAD, VERIFICACION Y VALIDACIÓN POR LA ARMADA

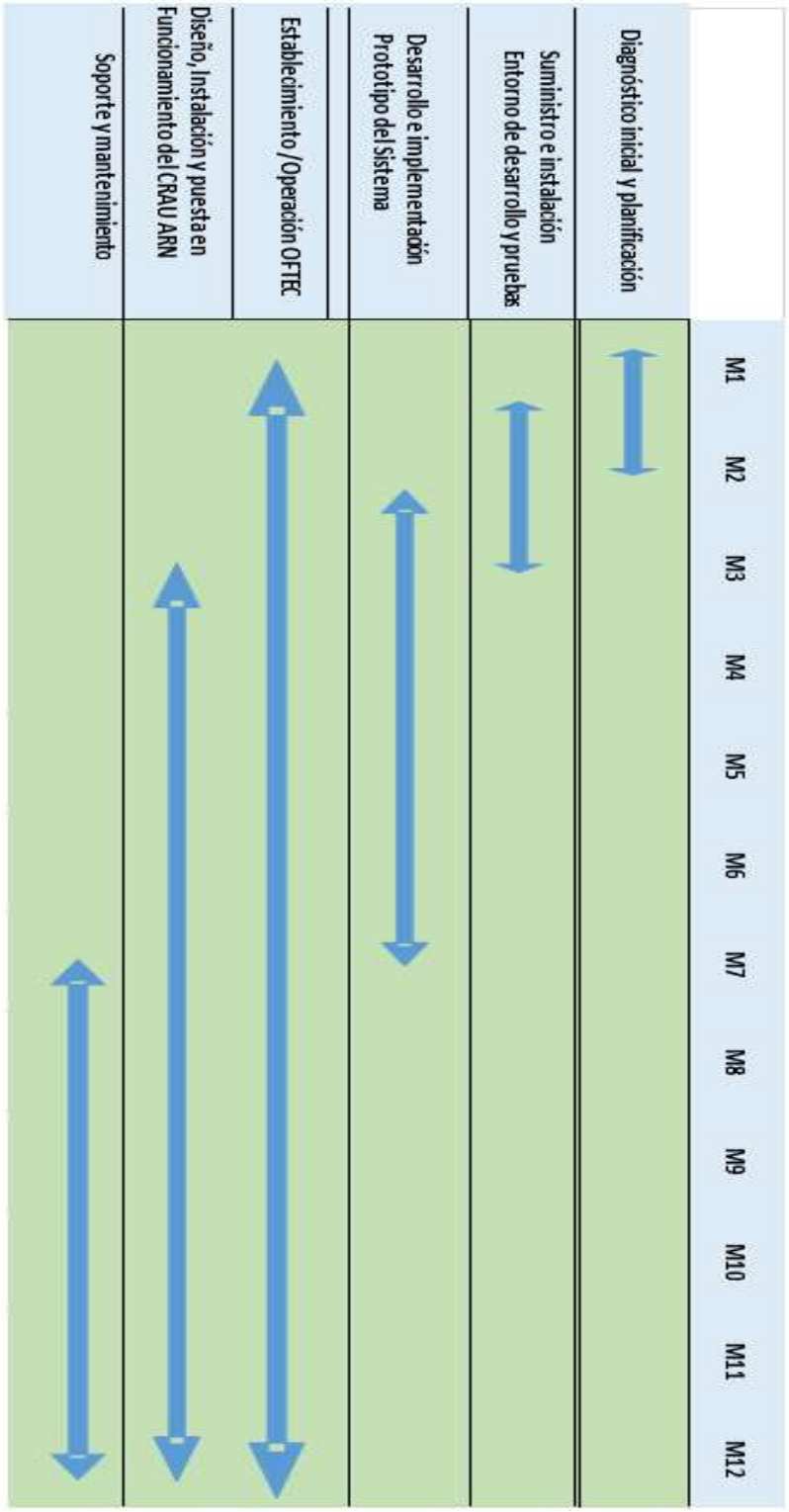
La Armada se reserva el derecho de realizar las inspecciones y comprobaciones que estime oportunas en los trabajos que se realicen al nuevo "Sistema de Seguridad Física Inteligente de la Armada", así como la realización de las correspondientes auditorias y verificar la implantación y cumplimiento de las instrucciones, normas y procedimientos de trabajo establecidos y aprobados.

ANEXOS

ANEXO I: *DEFINICION DE TERMINOS, ABREVIATURAS Y SIMBOLOS*

ARN	Área de Responsabilidad Norte
CESTIC	Centro de Sistemas y Tecnologías de la Información y las Comunicaciones
CPD	Centro de proceso de datos
CPI	Centro de Pruebas e integración
CRA	Centro receptor de alarmas
CRAU	Centro receptor de alarmas unificado
EGS	Entorno global de seguridad
I3D	Infraestructura Integral de Información del Ministerio de Defensa
NSA	Nivel de seguridad asignado
OSEFA	Oficina de seguridad física de la Armada
PAC	Plan de Aseguramiento de la Calidad
SAI	Sistema de alimentación ininterrumpida

ANEXO II: CALENDARIO TENTATIVO PARA ADAPTACIÓN. Fases 0 y 1.



HITOS

Este contrato tendrá seis (6) hitos para la Adaptación de la plataforma comercial previos a la aceptación del mismo (Fases 0 y 1), en los cuales se habrá de proporcionar un conjunto de entregables o prestaciones, que más adelante se especifican. A la finalización del contrato el sistema estará dimensionado para la futura instalación de elementos prevista en los apéndices.

De acuerdo con lo dispuesto en el artículo 95.5 de la Ley de Contratos de las Administraciones Públicas (modificada por Real Decreto Legislativo 2/2000 de 16 de Junio), el contrato podrá ser resuelto en caso de incumplimiento de los hitos por parte del contratista. Las fechas límite de cumplimiento de los hitos son las siguientes (T_0 es la fecha de firma del contrato):

FASES 0 y 1

HITOS	FECHA LIMITE DE CUMPLIMIENTO
1	Antes del T_0 + 1 mes
2	Antes del T_0 + 3 meses
3	Antes del T_0 + 5 meses
4	Antes del T_0 + 7 meses
5	Antes del T_0 + 9 meses
6	Antes del T_0 + 11 meses
Aceptación del sistema. Fin Fase1	Antes del T_0 + 12 meses

Antes de la fecha de cada hito se tendrá que entregar con una antelación de 15 días como mínimo o lo establecido en el Plan de entregas, la documentación correspondiente al Plazo parcial.

FASE 2

Comenzará al finalizar la FASE 1.

La fecha límite del contrato será T_0 + 18 meses.

Los entregables se relacionan en grandes conjuntos y con nombres genéricos, debido a que durante el diseño se identificarán los elementos de configuración específicos a desarrollar. Se adoptará metodología ISO 12207 o equivalente para el ciclo de vida del desarrollo.

Hito 1. Diagnóstico inicial, planificación y adquisición de licencias de software.

Entregables/Prestaciones:

- Plan de Trabajos
- Plan de Control de la Configuración
- Plan de Calidad
- Plan de Documentación
- Nombramiento 100 % personal Oficina Técnica de Supervisión y Operación.
- Entrega licencias software

Hito 2. Suministro e instalación Entorno de implementación, actualización y pruebas del sistema. Integración

Entregables/Prestaciones:

- Informe de Entorno de implementación, actualización y pruebas del sistema en funcionamiento.
- Confirmación de calendario.

Hito 3. Adaptación e implementación del Sistema. Establecimiento /Operación OFTESO

Entregables/Prestaciones:

- Informe de Estado de Avance del Proyecto. Finalizadas obras civiles de infraestructura necesarias para implantación elementos del sistema.

Hito 4. Diseño, Instalación y puesta en Funcionamiento del CRAU ARN
Entregables/Prestaciones:

- Informe de Estado de Avance del Proyecto. Avance 50 % instalación de elementos del sistema finalizado.

Plazo parcial 5. Diseño, Instalación y puesta en Funcionamiento del CRAU ARN

Entregables/Prestaciones:

- Informe de Estado de Avance del Proyecto. Alcance: 80% instalación de elementos del sistema finalizado.
- Plan de Formación validado.

Hito 6. Soporte y mantenimiento

Entregables/Prestaciones:

- Manuales de operación y usuario del Sistema
- Manuales de administración, mantenimiento y ciclo de vida.
- Documentación de apoyo a los cursos de formación
- Informe de Estado de Avance del Proyecto. Alcance: Listo para pruebas.

Aceptación del Sistema

Entregables/Prestaciones:

- Certificación de corrección de errores encontrados durante las pruebas.
- Informe Final del Proyecto. Alcance: Final tras pruebas.

Además, en todos los hitos se deberá incluir necesariamente*:*

- La entrega de una copia electrónica con toda la documentación (textual, gráfica, planos, etc.) generada durante el proyecto, con las restricciones respecto a su formato especificadas en la sección "Requisitos de la Documentación".

Códigos fuente del software y firmware generados por el contratista durante la ejecución de los trabajos y relacionados con los mismos, siempre que hayan sido desarrollados con cargo al programa

ANEXO III: FASE 1

En este apartado se presenta la relación de unidades y especificaciones técnicas de la fase 1, a efectos de que el licitador pueda evaluar la viabilidad de la integración geográfica y temporal.

El desarrollo de la implementación de plataforma integrará los siguientes EGS del AOR Norte:

ENTORNO GLOBAL DE SEGURIDAD	OBSERVACIONES	
EGC ARSENAL DE FERROL	CRA	SE PODRÁN INCORPORAR UAS DE SUPERFICIE COMO PRUEBA PILOTO
(EGC E.N. LA GRAÑA)	-	
EGU DEPOSITOS VISPÓN	C/C	
EGU TERCIO NORTE	CRAU	
EGC POLVORINES DE MOUGÁ	CRA	SE PODRÁN INCORPORAR UAS TERRESTRES Y AÉREOS COMO COMO PRUEBA PILOTO
EGC ESCUELA NAVAL MILITAR	CRA	SE PODRÁN INCORPORAR SISTEMAS C-UAS

Continúa el detalle y descripción de los citados EGS en documento CONFIDENCIAL separado por contener datos clasificados.

ANEXO IV: FASE 2

IMPLEMENTACIÓN PLATAFORMA EN EL AOR NORTE

Una vez aprobada la adaptación de la plataforma comercial, la solución se implementará en el resto de EGS del AOR Norte, siguiendo los requisitos técnicos especificados en el apéndice A de este anexo IV y mismos criterios establecidos en la fase 1 para las condiciones mínimas técnicas y los requisitos técnicos de las cámaras.

El listado de Unidades integradas del resto del AOR Norte es el siguiente:

ENTORNO GLOBAL DE SEGURIDAD		OBSERVACIONES
UNIDADES DEL EGC ARFER NO INLCUIDAS EN FASE 1		
	EGU JEFATURA COMARFER	C/C
	EGU JEFATURA 31 ESCUADRILLA	C/C
	EGU RESIDENCIA LOGISTICA LA CORTINA	C/C
	EGU CECISFER	C/C
	EGU ALA BALANDRA	C/C
	EGU SC JURIDICA	ALARMAS REMOTADAS
	EGU OAP	ALARMAS REMOTADAS
	EGU MUSEO NAVAL	C/C
EGC E.N. LA GRAÑA		CRA
	EGU CG FUPRO	C/C
	EGU ESCUELA ESPECIALIDADES DE LA E.N. DE LA GRAÑA	INCLUIDO EN CRA EGC
	EGU UNIDAD DE BUCEO	C/C
EGU ESCUELA DE ESPECIALIDADES A. ESCAÑO		CRA
EGU REPUESTOS CARANZA		C/C
EGU INTENDENCIA		ALARMAS REMOTADAS
EGU EDIFICIO ICO (NAVANTIA)		C/C
EGU INSTALACIONES DEPORTIVAS		C/C
EGC CDSA EL MONTÓN		C/C
	EGU RLA EL MONTÓN	C-C

ENTORNO GLOBAL DE SEGURIDAD	OBSERVACIONES
EGC PALACIO DE CAPITANÍA	C/C
EGU ARCHIVO NAVAL	PREVISTO TRASLADO A ELS HERRERÍAS
EGU PARQUE AUTOMÓVILES	C/C (PREVISTO UNO SOLO)
EGU FACTORÍA SUBSISTENCIAS	
EGU RESIDENCIA GALATEA	C/C
EGC C.N. DEL MIÑO	C/C
EGU C.N. DE BILBAO	C/C
EGU C.N. DE SAN SEBASTIAN	C/C
EGU A.N. DE BIDASOA	C/C
EGU C.N. DE SANTANDER	C/C
EGU C.N. DE VIGO	C/C
EGU C.N. DE GIJÓN	C/C
EGU RME TTE. GENERAL BARROSO	C/C
EGU CENTRO DE EDUCACIÓN PRIMARIA J.S. ELCANO	ALARMAS REMOTADAS

Continúa el detalle y descripción de los citados entornos en documento CONFIDENCIAL separado por contener datos clasificados.

El CC. Jefe del Área de Seguridad de Instalaciones en Tierra

FIRMA EN ORIGINAL

-Alfonso García de Paredes y Ucero-